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 these 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 also can 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.

Topics

Are You a First-Time AWS Artifact User?

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

Accessing AWS Artifact

AWS Artifact provides a web-based user interface, the AWS Artifact console. If you've signed up for an AWS account and have contacted AWS for these documents before, you can access the AWS Artifact console by signing into the AWS Management Console and choosing Artifact from the console home page.

Securing Your Documents

Audit artifacts are confidential documents, 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 Non-Disclosure Agreement (NDA) before you can download documents. Each document download has a unique, traceable watermark.

Audit artifacts should be shared only with those you trust. We strongly recommend that you use a secure document sharing service, such as Amazon WorkDocs, to share documents with others. Do not send these documents over email or upload them to an unsecure site.

Pricing for AWS Artifact

AWS Artifact is provided to you free of cost.

Setting Up AWS Artifact

When you sign up for Amazon Web Services (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 identity and 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 User (p. 3).

Topics
- Sign Up for AWS (p. 3)
- Create an IAM User (p. 3)

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 choose **Create an AWS Account**.
2. Follow the online instructions.

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

Create an IAM User

When you sign up for AWS, you provide an email address and password that is 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 logging 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 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 he or she needs to work with specific documents. For more information, see Step 1: Create an Admin Group and Add an IAM User (p. 5).

If you already manage user identities outside of 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

AWS Artifact offers a number of documents for downloading. Different documents require different permissions, which are controlled by a combination of IAM policies and whitelisting. This Getting Started tutorial shows you how to set up permissions and download reports by completing the following steps:

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

In this step, you create an Administrators group and add yourself as an IAM user to the group.

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

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users**, and then choose **Add user**.
3. For **User name**, type a user name, such as `Administrator`. The name can consist of letters, digits, and the following characters: plus (+), equal (=), comma (,), period (.), at (@), underscore (_), and hyphen (-). The name is not case sensitive and can be a maximum of 64 characters in length.
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 select 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. Choose **Create group**.
8. In the **Create group** dialog box, type the name for the new group. The name can consist of letters, digits, and the following characters: plus (+), equal (=), comma (,), period (.), at (@), underscore (_), and hyphen (-). The name is not case sensitive and can be a maximum of 128 characters in length.
9. For **Filter**, choose **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: 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 for Administering AWS Resources.
You can repeat the preceding steps to add other IAM users to the admin group.

Step 2: Create an IAM Policy

In step 1, you created an admin group and added yourself to the group as an IAM user. You can repeat step 1 to add other IAM users to the admin group at any time. In step 2, you create a permissions policy for a non-admin group that gives the IAM users in the group access to the AWS Artifact documents.

To create an IAM policy

1. Sign in to 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 the following:

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

This policy grants access to ISO certification reports, PCI compliance reports, and Service Organization Control (SOC) reports. 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 non-admin group.

Step 3: Create IAM Users

In the preceding steps, you created an admin group, added yourself to the group as an IAM user, and created a permissions policy. You can add other IAM users to the group at any time. You also can create non-admin groups and add IAM users to those groups. Now that you have created an admin user and a policy, create a group of IAM users and add each of the people that you want to have access to AWS Artifact documents. To do so, use the procedure from Step 1: Create an Admin Group and Add an IAM User (p. 5), using the policy that you just created in step two instead of **AdministratorAccess**.

Step 4: Download a Document

Now that you have set up your IAM users and policies, you can download a document by following the procedure in Downloading Documents (p. 8).

Downloading Documents

You can download documents from the AWS console. When you download a document from AWS Artifact, the documented is generated specifically for you, and every document has a unique watermark. For this reason, you should share the documents only with those you trust. Do not email the documents as attachments, and do not share them online. To share a document, use a secure sharing service such as Amazon WorkDocs. Some documents require you to sign an NDA before you can download them.

To download a document, you must have the appropriate permissions. For more information about getting started, see Getting Started.

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 the document to download.
3. Read the **Terms and Conditions** for the document. You might be asked to sign an NDA to download the document.

   Note
   The **Nondisclosure Agreement** is a legally binding contract. We recommend that you read it closely.
4. After you have read the **Terms and Conditions**, choose **Accept and Download**. AWS Artifact generates your file and opens a dialog box.
5. In the document dialog box, 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 Documents

When you sign up for AWS Artifact, you are automatically granted permissions to download some documents. If you need to request access to another listed document, ask your account admin (if you're an IAM user) and include the ARN for the document that you are requesting access for, or request additional permissions from AWS (if you're an admin) using the provided form.

Document History for AWS Artifact

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

- **Latest documentation update:** November 30th, 2016

Change	Description	Date
Release of the documentation	The first release of the documentation. Includes details for setting up, getting started, and downloading a document.	November 30, 2016

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the *AWS General Reference*.