Buyer Guide

AWS Marketplace

AWS Marketplace: Buyer Guide

Table of Contents

What is AWS Marketplace?

AWS Marketplace is a curated digital catalog that you can use to find, buy, deploy, and manage third-party software, data, and services that you need to build solutions and run your businesses. AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, IoT, business intelligence, database, and DevOps. AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. In addition, AWS Marketplace includes data products available from AWS Data Exchange.

You can quickly launch pre-configured software with just a few clicks, and choose software solutions in Amazon Machine Images (AMIs) and software as a service (SaaS) formats, as well as other formats. Additionally, you can browse and subscribe to data products. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and a Bring Your Own License (BYOL) model. All of these pricing options are billed from one source. AWS handles billing and payments, and charges appear on your AWS bill.

You can use AWS Marketplace as a buyer (subscriber) or as a seller (provider), or both. Anyone with an AWS account can use AWS Marketplace as a consumer and can register to become a seller. A seller can be an independent software vendor (ISV), value-added reseller, or individual that has something to offer that works with AWS products and services.

> **Note**
>
> Data product providers need to meet the AWS Data Exchange eligibility requirements. For more information, see Providing Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Every software product in AWS Marketplace has been through a curation process. On the product page, there can be one or more offerings for the product. When the seller submits a product in AWS Marketplace, they define the price of the product, and the terms and conditions of use. Buyers agree to the pricing, and terms and conditions set for the offer.

In AWS Marketplace, the product can be free to use or can have an associated charge. The charge becomes part of your AWS bill, and after you pay, AWS Marketplace pays the seller.

> **Note**
>
> When buying from some non-US sellers, you may also receive a tax invoice from the seller. For more information, see AWS Marketplace Sellers on Amazon Web Service Tax Help.

Products can take many forms. For instance, a product can be offered as an Amazon Machine Image (AMI) that is instantiated using your AWS account. The product could also be configured to use AWS CloudFormation templates for delivery to the consumer. The product could also be software as a service (SaaS) offerings from an ISV, or a web ACL, set of rules, or conditions for AWS WAF.

You can purchase software products at the listed price using the ISV's standard end user license agreement (EULA) or from a private offer with custom pricing and EULA. You can also purchase products under a standard contract with specified time or usage boundaries.

After the product subscriptions are in place, you can use AWS Service Catalog to copy the product and manage how the product is accessed and used in your organization. For more information, see Adding AWS Marketplace Products to Your Portfolio in the *AWS Service Catalog Administrator Guide*.

Contract structure in AWS Marketplace

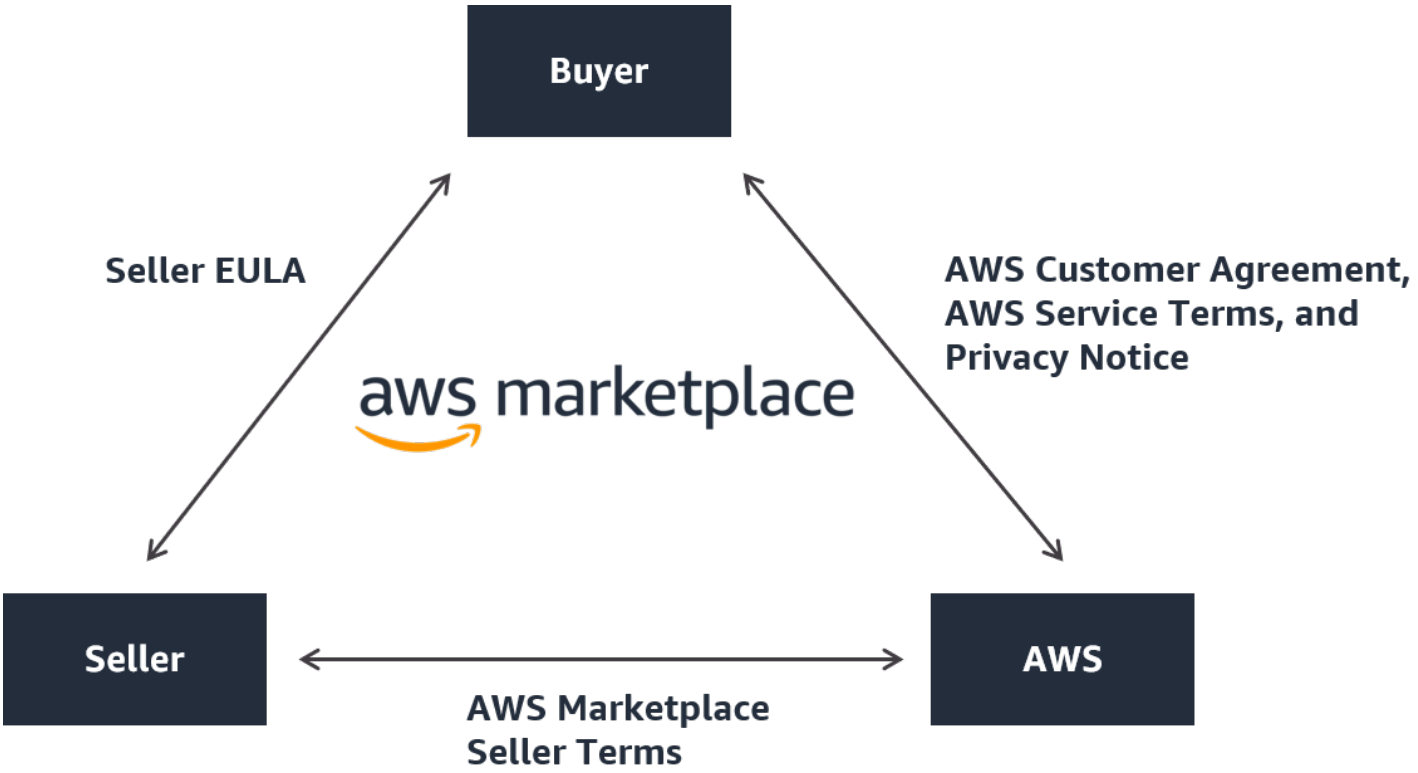
Usage of the software, services, and data products sold on AWS Marketplace is governed by agreements between buyers and sellers. AWS is not a party to these agreements.

As the buyer, your use of AWS Marketplace is governed by the AWS Service Terms, the AWS Customer Agreement, and the Privacy Notice.

Seller agreements include the following:

- The seller's EULA is located on the product listing page for public software listings on AWS Marketplace. Many sellers use the Standard Contract for AWS Marketplace (SCMP) as their default EULA. They can also use the SCMP as the basis for negotiations in private offers and use the amendment template to modify the SCMP. Private offers can also include custom contract terms negotiated between the parties.
- AWS Marketplace Seller Terms govern the seller's activity in AWS Marketplace.

The following graphic shows the contract structure for AWS Marketplace.



EULA updates

Sellers have the option to update the EULA for each of their products. The effective date of any updates will depend on your EULA, the offer type, and the pricing model.

The following table provides information on when a new EULA will take effect.

> **Note**
>
> If you and the seller have a custom agreement, the following may not be applicable.

Offer type	Pricing model	When updated EULA takes effect
Public	Usage	You cancel your subscription and resubscribe.

Offer type	Pricing model	When updated EULA takes effect
Public	Contract	Your current contract ends and renews into a new public offer contract.
Public	Contract with consumption	Your current contract ends and renews into a new public offer contract.
Private	Usage	Your current private offer expires and auto-renews into a new public offer contract. Renewals to the private offer are dependent on the specific private offer.
Private	Contract	Your current private offer expires and you resubscribe to the public offer or to a new private offer. Renewals to the private offer are dependent on the specific private offer.
Private	Contract with consumption	Your current private offer expires and you resubscribe to the public offer or to a new private offer. Renewals to the private offer are dependent on the specific private offer.

Standard contracts for AWS Marketplace

As you prepare to purchase a product, review the associated EULA or standardized contract. Many sellers offer the same standardized contract on their listings, the Standard Contract for AWS Marketplace (SCMP). AWS Marketplace developed the SCMP in collaboration with buyer and seller

communities to govern usage and define the obligations of buyers and sellers for digital solutions. Examples of digital solutions include server software, software as a service (SaaS), and artificial intelligence and machine learning (AI/ML) algorithms.

Instead of reviewing custom EULAs for each purchase, you only need to review the SCMP once. The contract terms are the same for all products that use the SCMP.

Sellers may also use the following addendums with the SCMP:

- Enhanced Security Addendum – Supports transactions with elevated data security requirements.
- HIPAA Business Associate Addendum – Supports transactions with Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance requirements.

To find product listings that offer standardized contracts, use the **Standard Contract** filter when searching for products. For private offers, ask the seller if they can replace their EULA with the SCMP and apply agreed upon amendments as necessary to support transaction-specific requirements.

For more information, see Standardized Contracts in AWS Marketplace.

Using AWS Marketplace as a buyer

As a buyer, you go to AWS Marketplace to search, filter, and navigate to a product that runs on Amazon Web Services.

When you choose a software product, you are taken to the product's page. The page has information about the product, pricing, usage, support, and product reviews. To subscribe to the software product, you sign in to your AWS account and are taken to a subscription page that has the EULA, terms and conditions of usage, and any options available for customizing your subscription.

AWS Marketplace purchases made by your accounts based in Europe, the Middle East, and Africa (excluding Turkey and South Africa) from EMEA-eligible sellers are facilitated by Amazon Web Services EMEA SARL.

For customers in certain countries, Amazon Web Services EMEA SARL charges local value-added tax (VAT) on your AWS Marketplace purchases. For more information about taxes, see the AWS Marketplace Buyers Tax help page.

For more information about Amazon Web Services EMEA SARL, see the Amazon Web Services EMEA SARL FAQs.

Customers who transact with EMEA-eligible sellers receive an invoice from Amazon Web Services EMEA SARL. All other transactions continue to go through AWS Inc. For more information, see Paying for products.

After the subscription is processed, you can configure fulfillment options, software versions, and AWS Regions where you want to use the product, and then launch the software product. You can also find or launch your products by visiting Your Marketplace Software on the AWS Marketplace website, from your AWS Marketplace or Amazon Elastic Compute Cloud (Amazon EC2) console, or through the Service Catalog.

For more information about product categories available using AWS Marketplace, see Product categories.

For more information about delivery methods for software products in AWS Marketplace, see:

- AMI-based products
- Container products
- Machine learning products
- Professional services products
- SaaS products
- Data products – See What is AWS Data Exchange? in the *AWS Data Exchange User Guide*

Software and services on AWS Marketplace

AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. You can select commercial software from well-known sellers, as well as many widely used open source offerings. When you find products you want, you can buy and deploy that software to your own Amazon EC2 instance with 1-Click. You can also use AWS CloudFormation to deploy a topology of the product.

Any AWS customer can shop on AWS Marketplace. Software prices and estimated infrastructure prices are displayed on the website. You can purchase most software immediately, using payment instruments already on file with AWS. Software charges appear on the same monthly bill as AWS infrastructure charges.

Notes

- Many business products are available in the AWS Marketplace, including both software as a service (SaaS) and server-based products. The server-based products might require technical knowledge or IT support to set up and maintain.
- The information and tutorials in Tutorial: Get started with Amazon EC2 Linux instances can help you learn Amazon EC2 basics.
- If you plan to launch complex topologies of AWS Marketplace products through AWS CloudFormation, Getting started with AWS CloudFormation can help you learn useful AWS CloudFormation basics.

AWS Marketplace includes the following categories of software:

- Infrastructure software
- Developer tools
- Business software
- Machine learning
- IoT
- Professional services
- Desktop Applications
- Data products

For more information, see Product categories.

Each major software category contains more specific subcategories. For example, the Infrastructure software category contains subcategories such as Application Development, Databases & Caching, and Operating Systems. Software is available as one of seven different product types, including Amazon Machine Images (AMIs) and software as a service (SaaS). For information about the different software types, see *Product types*.

To aid you in choosing the software you need, AWS Marketplace provides the following information:

- Seller details

- Software version
- Type of software (AMI or SaaS), and information about the AMI if applicable
- Buyer rating
- Price
- Product information

Differences between AWS Marketplace and Amazon DevPay

There are substantial differences between AWS Marketplace and Amazon DevPay. Both help customers buy software that runs on AWS, but AWS Marketplace offers a more comprehensive experience than Amazon DevPay. For software buyers, the key differences are the following:

- AWS Marketplace offers a shopping experience more like Amazon.com, simplifying discovery of available software.
- AWS Marketplace products work with other AWS features such as virtual private cloud (VPC) and can be run on Amazon Elastic Compute Cloud (Amazon EC2) Reserved Instances and Spot Instances, in addition to On-Demand Instances.
- AWS Marketplace supports software backed by Amazon Elastic Block Store (Amazon EBS), and Amazon DevPay does not.

Additionally, software sellers benefit from the marketing outreach and ease of discovery of AWS Marketplace.

Getting started as a buyer

The following topics outline the process of getting started with software products as an AWS Marketplace buyer.

Topics

For information about getting started with data products, see Subscribing to data products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Buying products

In AWS Marketplace, buying a product means that you have accepted the terms of the product as shown on the product detail page. This includes pricing terms and the seller's end user license agreement (EULA), and that you agree to use such product in accordance with the AWS Customer Agreement. You will receive an email notification to the email address associated with your AWS account for offers accepted in AWS Marketplace.

> **Note**
>
> AWS offers the option to request guided demonstrations for certain products on AWS Marketplace at no charge. If a guided demonstration is available, a **Request demo** button will display on the product detail page. To request a demo, choose the button and provide request details. You'll receive a confirmation email summarizing your request, and an AWS representative will contact you.

If the product has a monthly fee or is purchased with a subscription contract, you are charged the fee upon subscription. The subscription is prorated based on the time remaining in the month. No other charges are assessed until you take one of the following actions:

- Launch an Amazon Elastic Compute Cloud (Amazon EC2) instance with the product Amazon Machine Image (AMI).
- Deploy the product using an AWS CloudFormation template.
- Register the product on the seller's website.

If the product has an annual subscription option, you are charged the full annual fee upon subscription. This charge covers product usage base, with subscription renewal due on the anniversary of the original subscription date. If you don't renew at the end of the annual subscription period, the subscription converts to an hourly subscription at the current hourly rate.

For more information about data product subscriptions, see Subscribing to data products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Launching software

After buying software, you can launch Amazon Machine Images (AMIs) that contain it by using the 1-Click Launch view in AWS Marketplace. You can also launch it using other Amazon Web Services (AWS) management tools, including the AWS Management Console, the Amazon Elastic Compute Cloud (Amazon EC2) console, Amazon EC2 APIs, or the AWS CloudFormation console.

With the 1-Click Launch view, you can quickly review, modify, and then launch a single instance of the software with settings recommended by the software seller. The **Launch with EC2 Console** view provides an easy way to find the AMI identification number and other pertinent information that is required to launch the AMI using the AWS Management Console, Amazon EC2 APIs, or other management tools. The **Launch with EC2 Console** view also provides more configuration options than launching from the AWS Management Console, such as tagging an instance.

> **Note**
>
> If you're unable to access an instance type or AWS Region, it may not have been supported at the time the private offer was sent to you. Review your agreement details for more information. To obtain access to an instance or a Region, contact the seller and request an updated private offer. After you accept the new offer, you'll have access to the newly added instance or Region.

For AWS Marketplace products with complex topologies, the **Custom Launch** view provides a **Launch with CloudFormation Console** option that loads the product in the AWS CloudFormation console with the appropriate AWS CloudFormation template. You can then follow the steps in the AWS CloudFormation console wizard to create the cluster of AMIs and associated AWS resources for that product.

Tutorial: Buying an AMI-based software product

The following tutorial describes how to buy an Amazon Machine Image (AMI) product with AWS Marketplace.

Steps

Step 1: Creating an AWS account

You can browse the AWS Marketplace website (https://aws.amazon.com/marketplace) without being signed in to your AWS account. However, you must sign in to subscribe to or launch products.

You must be signed in to your AWS account to access the AWS Marketplace console. For information about how to create an AWS account, see Creating an AWS account in the *AWS Account Management Reference Guide*.

Step 2: Choosing your software

To choose your software

1. Navigate to the AWS Marketplace website.

> **Note**
>
> You can shop, subscribe, and launch new instances from either the public AWS Marketplace website, at https://aws.amazon.com/marketplace, or through AWS Marketplace in the AWS Management Console, at https://console.aws.amazon.com/marketplace/home#/subscriptions.
> The experiences across the two locations are similar. This procedure uses the AWS Marketplace website but notes any major differences when using the console.

2. The **Shop All Categories** pane contains the list of categories you can choose from. You can also choose software featured in the middle pane. For this tutorial, in the **Shop All Categories** pane, choose **Content Management**.
3. From the **Content Management** list, choose **WordPress Certified by Bitnami and Automattic**.
4. On the product details page, review the product information. The product details page includes additional information such as:

   - Buyer rating
   - Support offering
   - Highlights
   - Detailed product description
   - Pricing details for instance types in each AWS Region (for AMIs)
   - Additional resources to help you get started
5. Choose **Continue to Subscribe**.
6. If you aren't already signed in, you are directed to sign in to AWS Marketplace. If you already have an AWS account, you can use that account to sign in. If you don't already have an AWS account, see Step 1: Creating an AWS account.
7. Read the Bitnami offer terms, then choose **Accept Contract** to agree to the subscription offer.
8. It may take a moment for the subscription action to complete. When it does, you receive an email message about the subscription terms, and then you're able to continue. Choose **Continue to Configuration** to configure and launch your software.

Subscribing to a product means that you have accepted the terms of the product. If the product has a monthly fee, then upon subscription you are charged the fee, which is prorated based on the

time remaining in the month. No other charges will be assessed until you launch an Amazon Elastic Compute Cloud (Amazon EC2) instance with the AMI you chose.

> **Note**
>
> As a subscriber to a product, your account will receive email messages when a new version of the software you're subscribed to is published.

Step 3: Configuring your software

Because we chose software as an AMI, your next step is to configure the software, including selecting the delivery method, version, and AWS Region in which you want to use the software.

To configure your software

1. On the **Configure this software** page, select **64-bit (x86) Amazon Machine Image (AMI)** for the **Delivery Method**.
2. Choose the latest version available for **Software Version**.
3. Choose the **Region** you want to launch the product in, for example, **US East (N. Virginia)**.

   > **Note**
   >
   > As you make changes to your configuration, you might notice that the **Ami Id** at the bottom of the screen updates. The AMI ID has the form *ami-<identifier>*, for example, `ami-123example456`. Each version of each product in each Region has a different AMI. This AMI ID allows you to specify the correct AMI to use when launching the product. The **Ami Alias** is a similar ID that is easier to use in automation.
   > For more information about the AMI alias, see Using AMI aliases.

4. Select **Continue to Launch**.

Step 4: Launching your software on Amazon EC2

Before you launch your Amazon EC2 instance, you need to decide if you want to launch with 1-Click launch or if you want to launch using the Amazon EC2 console. 1-Click launch helps you launch quickly with recommended default options such as security groups and instance types. With 1-Click launch, you can also see your estimated monthly bill. If you prefer more options,

such as launching in an Amazon Virtual Private Cloud (Amazon VPC) or using Spot Instances, then you should launch using the Amazon EC2 console. The following procedures walk you through subscribing to the product and launching an EC2 instance using either 1-Click launch or the Amazon EC2 console.

Launching on Amazon EC2 using 1-Click launch

To launch on Amazon EC2 using 1-Click launch

1. On the **Launch this software** page, choose **Launch from website** in the **Choose Action** dropdown, and review the default settings. If you want to change any of them, do the following:

   - In the **EC2 Instance Type** dropdown list, choose an instance type.
   - In the **VPC Settings** and **Subnet Settings** dropdown lists, select the network settings you want to use.
   - In the **Security Group Settings**, choose an existing security group, or choose **Create New Based On Seller Settings** to accept the default settings. For more information about security groups, see Amazon EC2 security groups for Linux instances in the *Amazon EC2 User Guide*.
   - Expand **Key Pair**, and choose an existing key pair if you have one. If you don't have a key pair, you're prompted to create one. For more information about Amazon EC2 key pairs, see Amazon EC2 key pairs.
2. When you're satisfied with your settings, choose **Launch**.

   Your new instance is launched with the *WordPress Certified by Bitnami and Automattic* software running on it. From here, you can view the instance details, create another instance, or view all instances of your software.

Launching on Amazon EC2 Using Launch with EC2 Console

To launch on Amazon EC2 Using Launch with EC2 Console

1. On the **Launch on EC2** page, choose the **Launch with EC2 Console** view, and then select an AMI version from the **Select a Version** list.
2. Review the **Firewall Settings**, **Installation Instructions**, and **Release Notes**, and then choose **Launch with EC2 Console**.

3. In the EC2 console, launch your AMI using the Request Instance Wizard. Follow the instructions in Get started with Amazon EC2 Linux instances to navigate through the wizard.

Step 5: Managing your software

At any time, you can manage your software subscriptions in AWS Marketplace by using the **Manage Subscriptions** page of the AWS Marketplace console.

To manage your software

1. Navigate to the AWS Marketplace console, and choose **Manage subscriptions**.
2. On the **Manage subscriptions** page:
   - View your instance status by product
   - View your current monthly charges
   - Run a new instance
   - View seller profiles for your instance
   - Manage your instances
   - Link directly to your Amazon EC2 instance so you can configure your software

Step 6: Terminating your instance

When you've decided that you no longer need the instance, you can terminate it.

> **Note**
>
> You can't restart a terminated instance. However, you can launch additional instances of the same AMI.

To terminate your instance

1. Navigate to the AWS Marketplace console, and choose **Manage subscriptions**.
2. On the **Manage subscriptions** page, choose the software subscription that you want to terminate an instance of, and select **Manage**.
3. On the specific subscription page, choose **View instances** from the **Actions** dropdown list.

4. Select the **Region** that the instance you want to terminate is in. This opens the Amazon EC2 console and shows the instances in that Region in a new tab. If necessary, you can return to this tab to see the Instance ID for the instance to close.
5. In the Amazon EC2 console, choose the **Instance ID** to open the **Instance details page**.
6. From the **Instance state** dropdown list, choose **Terminate instance**.
7. Choose **Terminate** when prompted for confirmation.

   Termination takes a few minutes to complete.

For more information

For more information about product categories and types, see *Product categories* and *Product types*.

For more information about Amazon EC2, see the service documentation at Amazon Elastic Compute Cloud Documentation.

To learn more about AWS, see https://aws.amazon.com/.

Supported AWS Regions in AWS Marketplace

For software products, the seller chooses which AWS Regions to make their software available in, as well as the instance types. We encourage making products available in all available Regions and on all instance types that make sense. The AWS Marketplace website is available worldwide and supports the following Regions:

- North America
  - US East (Ohio)
  - US East (N. Virginia)
  - US West (N. California)
  - US West (Oregon)
  - AWS GovCloud (US-East)
  - AWS GovCloud (US-West)
  - Canada (Central)
  - Canada West (Calgary)

- Africa
  - Africa (Cape Town)

- South America
  - South America (São Paulo)

- EMEA
  - Europe (Frankfurt)
  - Europe (Ireland)
  - Europe (London)
  - Europe (Milan)
  - Europe (Paris)
  - Europe (Spain)
  - Europe (Stockholm)
  - Europe (Zurich)

- APAC
  - Asia Pacific (Hong Kong)
  - Asia Pacific (Hyderabad)
  - Asia Pacific (Jakarta)
  - Asia Pacific (Melbourne)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Osaka)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)

- Middle East
  - Israel (Tel Aviv)
  - Middle East (Bahrain)
  - Middle East (UAE)

For more information about supported Regions for data products, see AWS Data Exchange endpoints and quotas in the *AWS General Reference*.

Product categories

The AWS Marketplace website is organized into primary categories, with subcategories under each. You can search and filter based on the categories and subcategories.

Topics

Infrastructure Software

The products in this category provide infrastructure-related solutions.

Backup & Recovery

Products used for storage and backup solutions.

Data Analytics

Products used for data analysis.

High Performance Computing

High performance computing products.

Migration

Products used for migration projects.

Network Infrastructure

Products used to create networking solutions.

Operating Systems

Packaged Linux and Windows operating systems.

Security

Security products for your infrastructure.

Storage

Applications focused on job roles involved in storage.

DevOps

The products in this category provide tools focused on developers and developer teams.

Agile Lifecycle Management

Products used for Agile SDLM.

Application Development

Products used for application development.

Application Servers

Servers used for application development.

Application Stacks

Stacks used for application development.

Continuous Integration and Continuous Delivery

Products used for CI/CD.

Infrastructure as Code

Products used for infrastructure.

Issues & Bug Tracking

Products used by developer teams to track and manage software bugs.

Monitoring

Products used for monitoring operating software.

Log Analysis

Products used for logging and log analysis.

Source Control

Tools used to manage and maintain source control.

Testing

Products used for automated testing of software products.

Business Applications

The products in this category help you run your business.

Blockchain

Products used for blockchain.

Collaboration & Productivity

Products used to enable collaboration in your business.

Contact Center

Products used for enabling Contact Centers in your organization.

Content Management

Products focused on content management.

CRM

Tools focused on customer relationship management.

eCommerce

Products that provide eCommerce solutions.

eLearning

Products that provide eLearning solutions.

Human Resources

Products used for enabling Human Resources in your organization.

IT Business Management

Products used for enabling IT business management in your organization.

Business Intelligence

Products used for enabling business intelligence in your organization.

Project Management

Tools for project management.

Machine Learning

The products in this category provide machine learning algorithms and model packages that work with Amazon SageMaker.

ML Solutions

Machine learning solutions.

Data Labeling Services

Products that provide data labeling capability.

Computer Vision

Products that enable computer vision capability.

Natural Language Processing

Products that enable natural language processing capability.

Speech Recognition

Products that enable speech recognition capability.

Text

Products that enable text learning capability. Examples include classification, clustering, edit/processing, embedding, generation, grammar/parsing, identification, names and entity recognition, sentiment analysis, summarization, text-to-speech, and translation.

Image

Products that enable image analysis capability. Examples include 3D, captioning, classification, edit/processing, embedding/feature extraction, generation, grammar/parsing, handwriting recognition, human/faces, object detection, segmentation/pixel labeling, and text/OCR.

Video

Products that enable video analysis capability. Examples include classification, object detection, edit/processing, anomaly detection, speaker identification, motion, re-identification, summarization, text/captioning, and tracking.

Audio

Products that enable audio analysis capability. Examples include speaker identification, speech-to-text, classification, song identification, and segmentation.

Structured

Products that enable structured analysis capability. Examples include classification, clustering, dimensionality reduction, factorization models, feature engineering, ranking, regression, and time-series forecasting.

IoT

Products used to create IoT-related solutions.

Analytics

Analytical products for IoT solutions.

Applications

Application products for the IoT solutions space.

Device Connectivity

Products used to manage device connectivity.

Device Management

Products used to manage devices.

Device Security

Products used to manage security for your IoT devices.

Industrial IoT

Products focused on providing industrial-related IoT solutions.

Smart Home & City

Products used to enable smart home and smart city solutions.

Professional Services

The products in this category provide consulting services related to AWS Marketplace products.

Assessments

Evaluation of your current operating environment to find the right solutions for your organization.

Implementation

Help with configuration, setup, and deployment of third-party software.

Managed Services

End-to-end environment management on your behalf.

Premium Support

Access to guidance and assistance from experts, designed for your needs.

Training

Tailored workshops, programs, and educational tools provided by experts to help your employees learn best practices.

Desktop applications

The products in this category provide infrastructure-related solutions.

Desktop Applications

Desktop applications and utilities for general productivity and specific job role enablement.

AP and Billing

Applications used for job roles focused on accounts payable and billing.

Application and the Web

General purpose and web environment applications.

Development

Applications used for development.

Business Intelligence

Applications used by job roles focused on managing business intelligence.

CAD and CAM

Applications used by job roles focused on computer-aided design and manufacture.

GIS and Mapping

Applications used by job roles focused on GIS and mapping.

Illustration and Design

Applications for job roles focused on illustration and design.

Media and Encoding

Application used for job roles involved in media and encoding.

Productivity and Collaboration

Applications focused on enabling productivity and enabling collaboration.

Project Management

Application for project manager job roles.

Security/Storage/Archiving

Applications focused on job roles involved in security, storage, and data archiving.

Utilities

Utility-focused applications for various job roles.

Data Products

The products in this category are sets of file-based data. For more information, see the AWS Data Exchange User Guide.

Industries

Education & Research

Products aimed at providing education and research solutions.

Financial Services

Products that enable financial services in your organization.

Healthcare & Life Sciences

Products used in the healthcare and life sciences industries.

Media & Entertainment

Media-related products and solutions.

Industrial

Industry-related products and solutions.

Energy

Energy-related products and solutions.

Product types

AWS Marketplace includes popular open source and commercial software, as well as free and paid data products. These products are available in different ways: as individual Amazon Machine Images (AMIs), as a cluster of AMIs deployed through an AWS CloudFormation template, as software as a service (SaaS), as professional services, and as AWS Data Exchange data products.

For more details about these product types, see the following topics:

- AMI-based products (including AMI and private image products)
- Container products
- Machine learning products
- Professional services products
- SaaS products
- Data products

AMI-based products

An Amazon Machine Image (AMI) is an image of a server, including an operating system and often additional software, which runs on AWS.

The software listed in AWS Marketplace is only available to run on Amazon Elastic Compute Cloud (Amazon EC2). It's not available for download.

On AWS Marketplace, you can search for AMIs (with search suggestions), view product reviews submitted by other customers, subscribe and launch AMIs, and manage your subscriptions. All AWS Marketplace products have been verified for quality and pre-configured for 1-Click launch capability on Amazon Web Services (AWS) infrastructure.

Both AMI and software as a service (SaaS) product listings are from trusted sellers. AMI products run within a customer's AWS account. You retain more control over software configuration and over the servers that run the software, but you also have additional responsibilities regarding server configuration and maintenance.

The AWS Marketplace catalog contains a curated selection of open source and commercial software from well-known sellers. Many products on AWS Marketplace can be purchased by the hour.

The AMI catalog is a community resource where people and development teams can list and exchange software or projects under development, without having to go through extensive vetting. Listings in the community AMI catalog may or may not be from well-known sellers and generally have not undergone additional investigations.

An AWS Marketplace product contains one AMI for each AWS Region in which the product is available. These AMIs are identical except for their location. Additionally, when sellers update their product with the latest patches and updates, they may add another set of AMIs to the product.

Some AWS Marketplace products may launch multiple instances of an AMI because they're deployed as a cluster using AWS CloudFormation templates. This cluster of instances, along with additional AWS infrastructure services configured by the CloudFormation template, act as a single product deployment.

AWS CloudFormation template

Important

AWS Marketplace will discontinue the delivery method for multiple Amazon Machine Image (AMI) products using AWS CloudFormation templates in August 2024. Other AWS Marketplace products using CloudFormation, such as single AMI with CloudFormation, won't be affected.
Until August 2024, existing subscribers can launch new instances of their multiple AMI products using CloudFormation templates from AWS Marketplace. After the discontinuation, they won't be able to launch new instances. Any existing instances previously launched and running in Amazon Elastic Compute Cloud (Amazon EC2) won't be impacted and will continue to run.
If you have questions, contact AWS Support.

AWS CloudFormation is a service that helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. A CloudFormation template describes the various AWS resources that you want, such as Amazon Elastic Compute Cloud (Amazon EC2) instances or Amazon Relational Database Service (Amazon RDS) database instances. CloudFormation takes care of provisioning and configuring those resources for you. For more information, see Getting started with AWS CloudFormation.

Using AWS CloudFormation templates

Software sellers may offer CloudFormation templates to define a preferred deployment topology consisting of multiple AMI instances and other AWS resources. If a CloudFormation template is available for a product, it will be listed as a deployment option on the product listing page.

You can use an AMI to deploy a single Amazon EC2 instance. You can use a CloudFormation template to deploy multiple instances of an AMI that act as a cluster—along with AWS resources such as Amazon RDS, Amazon Simple Storage Service (Amazon S3), or any other AWS service—as a single solution.

Topics

AMI subscriptions in AWS Marketplace

In AWS Marketplace, some Amazon Machine Image (AMI)-based software products offer an annual subscription pricing model. With this pricing model, you make a one-time upfront payment and pay no hourly usage fee for the next 12 months. You can apply one annual subscription to an AWS Marketplace software product to one Amazon Elastic Compute Cloud (Amazon EC2) instance.

> **Note**
>
> For AMI hourly with annual pricing, the annual subscription covers only the instance types that you specify when purchasing. For example, `t3.medium`. Launching any other instance type will incur the hourly rate for that instance type based on the active subscription.

You can also continue to launch and run AWS Marketplace software products by using hourly pricing. Charges for using Amazon EC2 and other services from AWS are separate and in addition to what you pay to purchase AWS Marketplace software products.

If you change the Amazon EC2 instance type for hourly usage, your Amazon EC2 infrastructure will be billed according to your signed savings plan. However, the AMI license from AWS Marketplace will automatically change to hourly pricing.

If an AMI hourly product doesn't support annual pricing, the buyer can't purchase an annual subscription. If an AMI hourly product does support annual pricing, the buyer can go to the product's page in AWS Marketplace and purchase annual contracts. Each annual contract allows the buyer to run one instance without being billed the hourly rate. Contracts vary according to instance type.

Annual agreement amendments

With hourly annual (annual) plan amendments, you can amend your plan directly from the AWS Marketplace Management Portal. You can use amendments when you need to switch the AMI to run on an Amazon Elastic Compute Cloud (Amazon EC2) instance type with more vCPUs, or move to a more modern generation of CPU architecture. With amendments, you can make the following changes to your existing annual plan:

- Switch between Amazon EC2 instance type families
- Switch between Amazon EC2 instance type sizes
- Add a new instance type
- Increase the quantity of an existing instance type in the agreement

Any new Amazon EC2 instance types you add or switch to in the agreement will be co-termed to the current end-date of the plan, so that all instance types in the agreement are renewed at the same time.

You can make a change as long as the prorated cost of the change is greater than zero. The prorated cost of the newly added Amazon EC2 instances is based on the annual cost of the instance type adjusted for the remaining term of the agreement. When switching instance types, the prorated cost of the removed Amazon EC2 instance type is deducted from the prorated cost of the newly added Amazon EC2 instance type.

> **Note**
>
> Amendments are supported for all agreements made from public offers and agreements from private offers without installment plans.

Annual agreement amendment examples

Consider the follow examples related to annual agreement amendments. In the following examples, the customer signed a contract on January 1, 2024, for two units of m5.large instance types ($4000/year). The seller is paid $8,000, minus the listing fees.

Example 1: Switching to an instance type of equal value

Mid-year, the customer wants to switch one unit of the m5.large instance type to one unit of the r5.large instance type. The prorated cost of the switch is calculated by deducting the prorated cost of the instance removed (six months of m5.large - $2000) from the prorated cost of the instance added (six months of r5.large - $2000). The net cost is $0, so the amendment can occur.

Example 2: Switching to higher priced instance type

Mid-year, the customer wants to switch one unit of the m5.large instance type to one unit of the m5.2xlarge instance type. The prorated cost of the switch is calculated by deducting the prorated cost of the instance removed (six months of m5.large - $2000) from the prorated cost of instance added (six months of m5.2xlarge - $3000). The net cost is $1,000, so the amendment can occur.

Example 3: Switching to a single unit of a lower-priced instance type

Mid-year, the customer wants to switch one unit of the m5.large instance type to one unit of the c5.large instance type. The prorated cost of the switch is calculated by deducting the prorated cost of the instance removed (6 months of m5.large - $2000) from the prorated cost of instance added (6 months of c5.large - $1,500). The net cost is -$500 (less than $0), so the amendment can't occur.

Example 4: Switching to multiple units of a lower-priced instance type

Mid-year, the customer wants to switch one unit of the m5.large instance type to two units of the c5.large instance type. The prorated cost of the switch is calculated by deducting the prorated cost of the instance removed (six months of m5.large - $2000) from the prorated cost of instances added (six months of two c5.large - $3,000). The net cost is $1,000, so the amendment can occur.

Example 5: Adding a new instance type

Mid-year, the customer wants to add an additional unit of the m5.large instance type to the agreement. The prorated cost of this change is calculated as the prorated cost of the instance added (six months of m5.large - $2,000). The net cost is $2,000, so the amendment can occur.

Example 6: Removing an instance type

Mid-year, the customer wants to remove one unit of the m5.large instance type. The prorated cost of this change is calculated as the prorated cost of instance removed (six months of m5.large - $2,000). The net cost is -$2,000 (less than $0), so the amendment can't occur.

AMI products with contract pricing

Some sellers offer public Amazon Machine Image (AMI)-based software products with a contract pricing model. In that model, you agree to make a one-time upfront payment for discrete quantities of licenses to access the software product for a duration of your choice. You're billed, in advance, through your AWS account. For example, you might purchase 10 user access licenses and 5 administrative licenses for a year. You can choose to automatically renew the licenses.

In addition, some companies offer private AMI-based software products with a contract pricing model. A private offer typically has a fixed duration which you can't change.

You can purchase an AMI -based software product contract using the product's detail page on AWS Marketplace. If this option is available, **AMI with contract pricing** appears for **Delivery Method** on the product's detail page. When you make the purchase, you will be directed to the product's website for account setup and configuration. The usage charges will then appear on your regular AWS account billing report.

Subscribing to an AMI product with contract pricing public offer

To subscribe to a public offer AMI-based product with a contract pricing model

1. Sign in to AWS Marketplace and find a container-based software product with a contract pricing model.
2. On the **Procurement** page, view the **Pricing Information**.

   You can see the **Units** and the rate for each duration (in months).
3. Choose **Continue to Subscribe** to start the subscription.

   To save this product without subscribing, choose **Save to List**.
4. Create an agreement by reviewing the pricing information and configuring the terms for the software product.

   a. Choose the duration of the contract: **1 month**, **12 months**, **24 months**, or **36 months**

b. Under **Renewal Settings**, choose whether to automatically renew the contract.

c. Under **Contract options**, choose a quantity for each unit.

The total contract price is displayed under **Pricing details.**

5. After you have made your selections, choose **Create Contract**.

The **Total contract price** is charged to your AWS account. A license is generated in AWS License Manager.

> **Note**
>
> It can take up to 10 minutes for the subscription to process and a license to be generated in your AWS License Manager account for the software product.

Subscribing to an AMI product with contract pricing private offer

To subscribe to a private offer AMI-based product with a contract pricing model

1. Sign in to AWS Marketplace with your Buyer account.
2. View the private offer.
3. On the **Procurement** page, view the **Pricing Information**.

   You can see the **Units** and the rate for each duration (in months).
4. Choose **Continue to Subscribe** to start the subscription.
5. Create an agreement by reviewing the pricing information and configuring the terms for the software product.

   The duration of the contract is already set by the Seller and can't be modified.
6. Under **Contract options**, choose a quantity for each unit.
7. View the total contract price under **Pricing details**.

   You can also see the public offer by choosing **View Offer** under **Other Available Offers**.
8. After you have made your selections, choose **Create Contract**.

Note

It can take up to 10 minutes for the subscription to process and a license to be generated in your AWS License Manager account for the software product.

Accessing the software

To access the AMI-based software product

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page:
   a. Choose **Manage License** to view, grant access, and track usage of your entitlements in AWS License Manager.
   b. Choose **Continue to Configuration**.
3. On the **Launch** page, review your configuration and choose how you want to launch the software under **Choose Action**.
4. On the **Choose an Instance Type**, choose an Amazon Elastic Compute Cloud (Amazon EC2) instance, and then choose **Next: Configure Instance Details**.
5. On the **Configure Instance Details** page, for **IAM role,** choose an existing AWS Identity and Access Management (IAM) role from your AWS account.

   If you don't have an IAM role, choose the **Create new IAM role manually** link and follow the instructions.

   Note

   When you purchase a product with contract pricing, a license is created by AWS Marketplace on the AWS account that your software can check using the License Manager API. You will need an IAM role to launch an instance of the AMI-based product.
   The following IAM permissions are required in the IAM policy.

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

```
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
   ]
}
```

6. After the instance details are configured, choose **Review and Launch**.
7. On the **Review Instance Launch** page, select an existing key pair or create a new key pair, and then choose **Launch Instances**.

   The **Initiating Instance Launches** progress window appears.
8. After the instance is initiated, go to the EC2 dashboard, and under **Instances**, see that the **Instance state** displays **Running**.

Viewing a generated license

To view a generated license

1. Sign in to AWS License Manager with your AWS account.
2. Under **Granted licenses**, view all of your granted licenses.
3. Search licenses by entering a product SKU, recipient, or status in the **Search** bar.
4. Choose the **License ID** and view the **License details**.
5. You can view the **Issuer** (AWS/Marketplace)and the **Entitlements** (the units that the license grants the right to use, access, or consume an application or resource).

Modifying an existing contract

If they have an existing upfront commitment for an AMI product, AWS Marketplace buyers can modify some aspects of a contract. An AMI contract is supported through contract terms based

offers as opposed to hourly or annual flexible consumption pricing (FCP) offers. This feature is available only to applications that are integrated with AWS License Manager. Buyers can purchase additional licenses within the entitlement of the same offer in the current contract. However, buyers can't reduce the entitlement counts purchased in the contract. Buyers can also cancel the automatic subscription renewal if the option is enabled by the Seller.

> **Note**
>
> A flexible payment schedule (FPS) contract offer can't be modified. There are no entitlement changes available to the buyer for an FPS purchased contract. An entitlement is a right to use, access, or consume an application or resource. FPS offers are not changeable.

Manage your subscription

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page, select **Manage License**.
3. From the list, select **View Terms**.
4. In the **Contract options** section, increase your entitlements by using the arrows. You can't reduce the entitlement counts below the entitlements purchased.
5. The contract details and total price displays in the **Pricing details** section.

To cancel your automatic subscription renewal

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page, select **Manage License**.
3. On the **Subscription** page, locate the **Renewal Settings** section.
4. Ensure you understand the terms and conditions with cancellation.
5. Select the check box to cancel the automatic renewal.

Metering-enabled AMI products

Some products listed on AWS Marketplace are billed on usage measured by the software application. Examples of metered usage dimensions include Data usage, Host/Agent usage, or Bandwidth usage. These products require extra configuration to function correctly. An IAM role with the permission to meter usage must be associated with your AWS Marketplace Amazon Elastic Compute Cloud (Amazon EC2) instance at the time of launch. For more information about IAM roles for Amazon EC2, see IAM Roles for Amazon EC2.

Cost allocation tagging in AMI products

AWS Marketplace supports cost allocation tagging for Amazon Machine Image (AMI)-based software products. New and existing Amazon Elastic Compute Cloud (Amazon EC2) instance tags automatically populate against corresponding AWS Marketplace AMI usage. You can use activated cost allocation tags to identify and track AMI usage through AWS Cost Explorer, the AWS Cost and Usage Reports, AWS Budgets, or other cloud spend analysis tools.

The vendor that provided the AMI may also record other custom tags in the metering for AMI-based products, based on information specific to the product. For more details, see Cost allocation tagging.

You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.

Cost allocation tagging only tracks costs from the time when the tags were activated in the Billing and Cost Management console. Only AWS account owners, AWS Organizations management account owners, and users with the appropriate permissions can access the Billing and Cost Management console for an account. Regardless of whether you use cost allocation tagging, there's no change to how much you're billed. Whether you use cost allocation tags has no impact on the functionality of your AMI-based software products.

Tracking cost allocation tags for one AMI across multiple instances

Each launched Amazon EC2 instance for a AWS Marketplace AMI subscription has a corresponding AWS Marketplace software usage line item in the AWS Cost and Usage report. Your AWS Marketplace usage will always reflect the specific tags applied to the corresponding Amazon EC2

instance. This allows you to distinguish your AWS Marketplace usage costs based on the different tag values that were assigned, at an instance level.

You can also sum up your tag-based usage costs to equal the AMI software usage charge reflected in your bill with either the Cost Explorer or the AWS Cost and Usage report.

Finding budgets with cost allocated tagged instances

If you already have active budgets filtered on cost allocation tags over a number of Amazon EC2 instances in the Billing and Cost Management console, it might be difficult to find all of them. The following Python script returns a list of budgets which contain Amazon EC2 instances from the AWS Marketplace in your current AWS Region.

You can use this script to be aware of a potential impact to your budget, and where overruns might occur from this change. Note that the billed amount doesn't change, but the cost allocations will be reflected more accurately, which can impact budgets.

```
#! /usr/bin/python

import boto3

session = boto3.Session()
b3account=boto3.client('sts').get_caller_identity()['Account']
print("using account {} in region {}".format(b3account,session.region_name))


def getBudgetFilters(filtertype):
    '''
    Returns budgets nested within the filter values [filter value][budeget name].
    The filtertype is the CostFilter Key such as Region, Service, TagKeyValue.
    '''
    budget_client = session.client('budgets')
    budgets_paginator = budget_client.get_paginator('describe_budgets')
    budget_result = budgets_paginator.paginate(
        AccountId=b3account
    ).build_full_result()
    returnval = {}
    if 'Budgets' in budget_result:
        for budget in budget_result['Budgets']:
            for cftype in budget['CostFilters']:
                if filtertype == cftype:
                    for cfval in budget['CostFilters'][cftype]:
                        if cfval in returnval:
```

```
                            if not budget['BudgetName'] in returnval[cfval]:
                                returnval[cfval].append(budget['BudgetName'])
                        else:
                            returnval[cfval] = [ budget['BudgetName'] ]
    return returnval

def getMarketplaceInstances():
    '''
    Get all the AWS EC2 instances which originated with AWS Marketplace.
    '''
    ec2_client = session.client('ec2')
    paginator = ec2_client.get_paginator('describe_instances')
    returnval = paginator.paginate(
        Filters=[{
            'Name': 'product-code.type',
            'Values': ['marketplace']
        }]
    ).build_full_result()
    return returnval


def getInstances():
    mp_instances = getMarketplaceInstances()
    budget_tags = getBudgetFilters("TagKeyValue")
    cost_instance_budgets = []
    for instance in [inst for resrv in mp_instances['Reservations'] for inst in
 resrv['Instances'] if 'Tags' in inst.keys()]:
        for tag in instance['Tags']:
            # combine the tag and value to get the budget filter string
            str_full = "user:{}${}".format(tag['Key'], tag['Value'])
            if str_full in budget_tags:
                for budget in budget_tags[str_full]:
                    if not budget in cost_instance_budgets:
                        cost_instance_budgets.append(budget)
    print("\r\nBudgets containing tagged Marketplace EC2 instances:")
    print( '\r\n'.join([budgetname for budgetname in cost_instance_budgets]) )


if __name__ == "__main__":
    getInstances()
```

Example output

```
Using account 123456789012 in region us-east-2

Budgets containing tagged Marketplace EC2 instances:
EC2 simple
MP-test-2
```

Related topics

For more information, see the following topics:

- Using Cost Allocation Tags in the *AWS Billing User Guide*.
- Activating the AWS-Generated Cost Allocation Tags in the *AWS Billing User Guide*.
- Tagging Your Amazon EC2 Resources in the Amazon EC2 User Guide.

Using AMI aliases

An Amazon Machine Image (AMI) is identified with an `AMI ID`. You can use the `AMI ID` to indicate which AMI you want to use when launching a product. The `AMI ID` has the form `ami-<identifier>`, for example, ami-123example456. Each version of each product in each AWS Region has a different AMI (and different `AMI ID`).

When you launch a product from AWS Marketplace, the `AMI ID` is automatically filled in for you. Having the `AMI ID` is useful if you want to automate launching products from the AWS Command Line Interface (AWS CLI) or by using Amazon Elastic Compute Cloud (Amazon EC2). You can find the `AMI ID` when you configure your software at launch time. For more information, see Step 3: Configuring your software.

The `Ami Alias` is also in the same location as the `AMI ID`, when configuring your software. The `Ami Alias` is a similar ID to the `AMI ID`, but it's easier to use in automation. An `AMI alias` has the form `aws/service/marketplace/prod-<identifier>/<version>` , for example, `aws/service/marketplace/prod-1234example5678/12.2`. You can use this `Ami Alias` Id in any Region, and AWS automatically maps it to the correct Regional `AMI ID`.

If you want to use the most recent version of a product, use the term **`latest`** in place of the version in the `AMI alias` so that AWS chooses the most recent version of the product for you, for example, **`aws/service/marketplace/prod-1234example5678/latest`**.

Warning

Using the **`latest`** option gives you the most recently released version of the software. However, use this feature with caution. For example, if a product has versions 1.x and 2.x available, you might be using 2.x. However, the most recently released version of the product might be a bug fix for 1.x.

Examples of using AMI aliases

AMI aliases are useful in automation. You can use them in the AWS CLI or in AWS CloudFormation templates.

The following example shows using an AMI alias to launch an instance by using the AWS CLI.

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
--instance-type m5.xlarge
--key-name MyKeyPair
```

The following example shows a CloudFormation template that accepts the AMI alias as an input parameter to create an instance.

```
AWSTemplateFormatVersion: 2010-09-09

Parameters:
    AmiAlias:
        Description: AMI alias
        Type: 'String'

Resources:
    MyEC2Instance:
        Type: AWS::EC2::Instance
        Properties:
            ImageId: !Sub "resolve:ssm:${AmiAlias}"
            InstanceType: "g4dn.xlarge"
            Tags:
                -Key: "Created from"
                 Value: !Ref AmiAlias
```

Container products

Container products are standalone products fulfilled as container images. Container products can either be free or must be paid for using a seller-provided pricing option. Container products can be used with multiple container runtimes and services, including Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and even services running on your own infrastructure. For a complete list of supported runtimes and services with more information about each, see Supported services for container products.

You can discover, subscribe to, and deploy container products on the AWS Marketplace website or in the Amazon ECS console. You can deploy many products to Amazon ECS or Amazon EKS by using seller-supplied deployment templates, such as task definitions or Helm charts. Or, you can access container images directly from private Amazon Elastic Container Registry (Amazon ECR) repositories after you have subscribed to those products.

If a product has enabled QuickLaunch, you can use it to quickly test container products on an Amazon EKS cluster with just a few steps. QuickLaunch uses AWS CloudFormation to create an Amazon EKS cluster and launch container software on it. For more information about launching with QuickLaunch, see QuickLaunch in AWS Marketplace.

This section provides information about finding, subscribing to, and launching container products in AWS Marketplace.

Pricing models for paid container products

Paid container products must have one or more pricing models. Like with any other paid products in AWS Marketplace, you're billed for paid container products by AWS according to the pricing model. The pricing model might be a fixed monthly fee or an hourly price, monitored in seconds and prorated. Pricing details will be shown on the detail page and when you subscribe to the product.

The supported pricing models for container products in AWS Marketplace are as follows:

- A fixed monthly charge that provides unlimited usage.
- An upfront charge for usage of the product for the duration of a long term contract.
- A pay-as-you-go model (typically hourly) based on usage of the product.
- A pay-up-front model with contract pricing.

For more information about each model, see Container product pricing in the *AWS Marketplace Seller Guide*.

Overview of containers and Kubernetes

Containers, such as Docker containers, are an open-source software technology that provides an additional layer of abstraction and automation over virtualized operating systems such as Linux and Windows Server. Just as virtual machines are instances of server images, containers are instances of Docker container images. They wrap server application software in a file system that contains everything it needs to run: code, runtime, system tools, system libraries, and so on. With containers, the software always runs the same, regardless of its environment.

Analogous to Java virtual machines, containers require an underlying platform to provide a translation and orchestration layer while being isolated from the operating system and each other. There are different Docker-compatible runtimes and orchestration services that you can use with Docker containers, including Amazon ECS, which is a highly scalable, high-performance orchestration service for AWS, and Amazon EKS, which makes it easy to deploy, manage, and scale containerized applications using Kubernetes, an open source management and orchestration service.

Finding and subscribing to container products

Container products are products in AWS Marketplace that can be launched on container images. Container products include any product in AWS Marketplace in which the seller has provided a fulfillment option with a **Container image**, **Helm chart**, or **Add-on for Amazon EKS** delivery method. For more information about container product delivery methods, see Container product delivery methods.

Many launch environments, also known as supported services, are available for fulfillment options in container products. Launch environments include services such as Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and even your own self-managed infrastructure. For a complete list of available container product launch environments, see Supported services for container products.

Browse container products using the AWS Marketplace website

You can browse container products by using the AWS Marketplace website.

To browse container products using the AWS Marketplace website

1. Navigate to the AWS Marketplace search page.
2. Filter **Delivery method** by **Container image** or **Helm chart**.
3. (Optional) Filter **Supported services** to narrow the search results by the services that the product can be launched with.

After you find a product that you're interested in, choose the title to navigate to the product details page.

Container product details page

In the product details page in AWS Marketplace, you can find details about the product, including the following information:

- **Product Overview** – The overview includes a product description and the following information:
  - The product version that you're viewing.
  - A link to the seller's profile.
  - The product categories that this product belongs to.
  - The supported operating systems to run this software.
  - The delivery methods that are available for launching the software.
  - The supported services that this product can be launched on.
- **Pricing Information** – Products have free tiers, Bring Your Own License (BYOL), pay-up-front with contract pricing, or pay-as-you-go with either a fixed monthly or annual price, or an hourly price. For more information about pricing models, see Container product pricing.
- **Usage Information** – Included here are seller-provided fulfillment options with instructions to launch and run the software. Each product must have at least one fulfillment option and can have up to five. Each fulfillment option includes a delivery method and instructions to follow to launch and run the software.
- **Support Information** – This section includes details about how to get support for the product and its refund policy.
- **Customer Reviews** – Find reviews for the product from other customers or write your own.

To subscribe to a product, choose **Continue to Subscribe** on the product's details page. For more information about subscribing to products, see Subscribing to products in AWS Marketplace.

Subscribing to products in AWS Marketplace

To use a product, you must subscribe to it first. On the subscription page, you can view pricing information for paid products and access the end user license agreement (EULA) for the software.

For a product with container contract pricing, select your contract pricing and choose **Accept Contract** to proceed. This creates a *subscription* to the product, which provides an *entitlement* to use the software. It will take a minute or two for the subscription to complete. After you receive an entitlement to a paid product, you will be charged when you start using the software. If you cancel your subscription without terminating all running instances of the software, you will continue to be charged for any software usage. You might also incur infrastructure charges related to using the product. For example, if you create a new Amazon EKS cluster to host the software product, you will be charged for that service.

> **Note**
>
> For a walkthrough on how to subscribe to and deploy a container-based product, you can also refer to the following videos:
>
> - Deploying AWS Marketplace Containers on Amazon ECS Clusters (3:34)
> - Deploying AWS Marketplace Container-based Products using Amazon ECS Anywhere (5:07)
> - Managing Amazon EKS add-ons

Container product delivery methods

A product in AWS Marketplace is considered a container product if the seller has provided at least one fulfillment option with either a **Container image**, **Helm chart**, or **Add-on for Amazon EKS** delivery method.

Container image delivery method

For a fulfillment option with a **Container image** delivery method, use the seller-provided instructions to launch the product. This is done by pulling Docker images directly from the AWS Marketplace registry on Amazon Elastic Container Registry. For more information about launching with this delivery method, see Launching with a Container image fulfillment option.

Helm chart delivery method

For a fulfillment option with a **Helm chart** delivery method, use the seller-provided instructions or deployment template to launch the product. This is done by installing a Helm chart using the Helm CLI. You can launch the application on an existing Amazon EKS cluster, or a self-managed cluster on EKS Anywhere, Amazon Elastic Compute Cloud (Amazon EC2), or on-premises. For more information about launching with this delivery method, see Launching with a Helm fulfillment option.

Add-on for Amazon EKS delivery method

For a fulfillment option with an **Add-on for Amazon EKS** delivery method, use the Amazon EKS console or Amazon EKS CLI to launch the product. For more information about Amazon EKS add-ons, see Amazon EKS add-ons.

Supported services for container products

The following list includes all of the supported services for container products in AWS Marketplace. A *supported service* is a container service or environment where the product can be launched. A container product must include at least one fulfillment option that includes a delivery method with instructions to launch to one or more of the environments.

Amazon ECS

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast container management service that you can use to run, stop, and manage containers on a cluster. Your containers are defined in a task definition that you use to run individual tasks or tasks within a service. In this context, a service is a configuration that allows you to run and maintain a specified number of tasks simultaneously in a cluster. You can run your tasks and services on a serverless infrastructure that's managed by AWS Fargate. Alternatively, for more control over your infrastructure, you can run your tasks and services on a cluster of Amazon EC2 instances that you manage.

For more information about Amazon ECS, see What is Amazon Elastic Container Service in the *Amazon Elastic Container Service Developer Guide*.

Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that you can use to run Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control

plane or nodes. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications.

You can search for, subscribe to, and deploy third-party Kubernetes software using the Amazon EKS console. For more information, see Managing Amazon EKS add-ons in the *Amazon EKS User Guide*.

Self-managed Kubernetes

You can launch container products on self-managed Kubernetes clusters running in EKS Anywhere, Amazon ECS Anywhere, Amazon EC2, or on-premises infrastructure.

Amazon ECS Anywhere is a feature of Amazon ECS that you can use to run and manage container workloads on customer managed infrastructure. Amazon ECS Anywhere builds upon Amazon ECS to provide a consistent tooling and API experience across your container-based applications.

For more information, see Amazon ECS Anywhere.

EKS Anywhere is a service that you can use to create an Amazon EKS cluster on customer managed infrastructure. You can deploy EKS Anywhere as an unsupported local environment or as a production-quality environment that can become a supported on-premises Kubernetes platform.

For more information about EKS Anywhere, see the EKS Anywhere documentation.

Browse container products using the Amazon ECS console

You can also find container products in the Amazon ECS console. The navigation pane has links to discover new products from AWS Marketplace and to see existing subscriptions.

Canceling a subscription

To cancel a subscription to a product, use the **Your Software** page.

Container products with contract pricing

Some sellers offer public container-based software products with a contract pricing model, in which you agree to make a one-time upfront payment for discrete quantities of licenses to access the software product for a duration of your choice, have are billed, in advance, through your AWS account.

Example of purchasing different types of licenses in different quantities

For example, you might purchase 10 user access licenses and 5 administrative licenses for a year. You can choose to automatically renew the licenses.

In addition, some companies offer private container-based software products with a contract pricing model. A private offer typically has a fixed duration that you can't change.

You can purchase a container-based software product contract using the product's detail page on AWS Marketplace. If this option is available, **AMI with contract pricing** appears for **Delivery Method** on the product's detail page. When you make the purchase, you will be directed to the product's website for account setup and configuration. The usage charges will then appear on your regular AWS account billing report.

Subscribing to a container product with contract pricing public offer in AWS Marketplace

To subscribe to a public offer container-based product with a contract pricing model

> **Note**
>
> For information about subscribing using Amazon EKS, see Managing Amazon EKS add-ons.

1. Sign in to AWS Marketplace and find a container-based software product with a contract pricing model.
2. On the **Procurement** page, view the **Pricing Information**.

   You can see the **Units** and the rate against each duration (in months).
3. To start the subscription, choose **Continue to Subscribe**.

   To save this product without subscribing, choose **Save to List**.
4. Create an agreement by reviewing the pricing information and configuring the terms for the software product.

   a. Choose the duration of the contract: **1 month**, **12 months**, **24 months**, or **36 months**.

   b. Under **Renewal Settings**, choose whether to automatically renew the contract.

   c. Under **Contract options**, choose a quantity for each unit.

The total contract price is displayed under **Pricing details.**

5. After you've made your selections, choose **Create Contract**.

The **Total contract price** is charged to your AWS account and a license is generated in AWS License Manager.

> **Note**
>
> It can take up to 10 minutes for the subscription to process and a license to be generated in your License Manager account for the software product.

Subscribing to a container product with contract pricing private offer in AWS Marketplace

To subscribe to a private offer container-based product with a contract pricing model

> **Note**
>
> For information about subscribing using Amazon EKS, see Managing Amazon EKS add-ons.

1. Sign in to AWS Marketplace with your Buyer account.
2. View the private offer.
3. On the **Procurement** page, view the **Pricing Information**.

   You can see the **Units** and the rate for each duration (in months).
4. Choose **Continue to Subscribe** to start the subscription.
5. Create an agreement by reviewing the pricing information and configuring the terms for the software product.

   The duration of the contract is already set by the Seller and can't be modified.
6. Under **Contract options**, choose a quantity for each unit.
7. View the total contract price under **Pricing details**.

You can also see the public offer by choosing **View Offer** under **Other Available Offers**.

8. After you've made your selections, choose **Create Contract**.

> **Note**
>
> It can take up to 10 minutes for the subscription to process and a license to be generated in your License Manager account for the software product.

Accessing the software

To access the container-based software product

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page:
   a. Choose **Manage License** to view, grant access, and track usage of your entitlements in AWS License Manager.
   b. Choose **Continue to Configuration**.
3. On the **Launch** page, view the container image details and follow the provided directions.

   While creating an Amazon Elastic Container Service (Amazon ECS) cluster, you must add the following AWS Identity and Access Management (IAM) permissions to your IAM policy.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
```

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

Viewing a generated license

To view a generated license

1. Sign in to AWS License Manager with your AWS account.
2. Under **Granted licenses**, view all of your granted licenses.
3. Search licenses by entering a product SKU, recipient, or status in the **Search** bar.
4. Choose the **License ID** and view the **License details**.
5. You can view the **Issuer** (AWS/Marketplace) and the **Entitlements** (the units that the license grants the right to use, access, or consume an application or resource).

Modifying an existing contract

If they have an existing upfront commitment for a Container product, AWS Marketplace buyers can modify some aspects of a contract. A Container contract is supported through contract terms based offers as opposed to hourly or annual flexible consumption pricing (FCP) offers. This feature is available only to applications that are integrated with AWS License Manager. Buyers can purchase additional licenses within the entitlement of the same offer in the current contract. However, buyers can't reduce the entitlement counts purchased in the contract. Buyers can also cancel the automatic subscription renewal if the option is enabled by the Seller.

> **Note**
>
> A flexible payment schedule (FPS) contract offer can't be modified. There are no entitlement changes available to the buyer for an FPS purchased contract. An entitlement is a right to use, access, or consume an application or resource. FPS offers are not changeable.

Manage your subscription

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page, select **Manage License**.
3. From the list, select **View Terms**.
4. In the Contract options section, increase your entitlements using the arrows. You can't reduce the entitlement counts below the entitlements purchased.
5. The contract details and total price displays in the **Pricing details** section.

To cancel your automatic subscription renewal

1. On the AWS Marketplace console, navigate to **View Subscription** and view the license for the software product.
2. On the **Procurement** page, select **Manage License**.
3. On the **Subscription** page, locate the **Renewal Settings** section.
4. Make sure that you understand the terms and conditions with cancellation.
5. Select the check box to cancel the automatic renewal option.

Launching container software from AWS Marketplace

After you have an active subscription to a container product in AWS Marketplace, the next step is to launch the software. To launch the software, follow the instructions included in one of the fulfillment options provided by the seller. In AWS Marketplace, a *fulfillment option* is an optional seller-provided procedure for launching their product in your environment. For container products, the seller can provide up to four fulfillment options, which can use different delivery methods and represent different configurations for the software. For example, a seller might create one fulfillment option that's used for testing the product, and another to be deployed at scale within an enterprise.

You can see which fulfillment options are available in the **Usage Information** section of the product details page in AWS Marketplace. Each fulfillment option includes information about which services are supported and provides software version details. Examples of services include Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon

EKS). You can choose **Usage instructions** for documentation from the seller about how to use the product, such as how to sign in to a web server, or post-launch configuration.

> **Note**
>
> For a walkthrough on how to subscribe to and deploy a container-based product, you can also refer to the following videos:
>
> - Deploying AWS Marketplace Containers on Amazon ECS Clusters (3:34)
> - Deploying AWS Marketplace Container-based Products using Amazon ECS Anywhere (5:07)

Deploying AWS Marketplace Container-Based Products Using ECS Anywhere

Launch container software from AWS Marketplace

To launch container software from AWS Marketplace

1. Sign in to AWS Marketplace.
2. Browse AWS Marketplace, and find the product that contains the software that you want to launch. You must have a subscription to the product to launch its software. For information about finding and subscribing to container products in AWS Marketplace, see Finding and subscribing to container products.
3. Choose **Continue to Subscribe** on the product details page.
4. Choose **Continue to Configuration**. If you don't see the button, you might have to accept terms first, or you might not have a subscription to the product.
5. In **Fulfillment option**, select a fulfillment option from the seller-provided list of options. After selecting a fulfillment option, you can see the services that you can launch in **Supported services**. For more information about fulfillment options, see Container product fulfillment options.
6. Choose **Continue to Launch**.
7. Follow the instructions provided by the seller to launch the product. The instructions are different for each fulfillment option. For more information, see Launching with a Container image fulfillment option or Launching with a Helm fulfillment option.
8. *Optional* - Choose **Usage instructions** for documentation from the seller about how to configure and use the product after launching.

Container product fulfillment options

You can see the fulfillment options that are available in the **Usage Information** section of a product's detail page. Alongside the fulfillment options provided by the seller, AWS Marketplace includes instructions for pulling the Docker images directly from Amazon Elastic Container Registry (Amazon ECR).

Because fulfillment options are provided by the seller, their names and content will be different for each product in AWS Marketplace. Although the methods are unique to each product and seller, each fulfillment option must have a *delivery method*. You can think of a delivery method as a fulfillment option type. The three available delivery methods for container products are **Container image**, **Helm chart**, and **Add on for Amazon EKS**.

Launching with a Container image fulfillment option

For a fulfillment option with a **Container image** delivery method, use the seller-provided instructions to launch the product. This is done by pulling Docker images directly from Amazon ECR. The general steps to launch the product are as follows:

1. Verify that you have installed the latest versions of the AWS Command Line Interface (AWS CLI) and Docker. For more information, see Using Amazon ECR with the AWS CLI in the *Amazon Elastic Container Registry User Guide*.
2. Authenticate your Docker client to your Amazon ECR registry. The steps to do this will depend on your operating system.
3. Pull all of the Docker images using the provided Amazon ECR image Amazon Resource Name (ARN). For more information, see Pulling an image in the *Amazon Elastic Container Registry User Guide*.
4. Review any usage instructions or external links provided by the seller for information about using the product.

Launching with a Helm fulfillment option

For a fulfillment option with a **Helm** delivery method, use the seller-provided instructions to launch the product. This is done by installing a Helm chart using the Helm CLI. You can launch the application on an existing Amazon EKS cluster, or a self-managed cluster on EKS Anywhere, Amazon Elastic Compute Cloud (Amazon EC2), or on-premises.

> **Note**
>
> Your launch environment must use Helm CLI version 3.7.1. For a list of Helm versions, see Helm releases on GitHub.

If the seller has enabled QuickLaunch, you can use it to launch the application. QuickLaunch is a feature in AWS Marketplace that uses AWS CloudFormation to create an Amazon EKS cluster and launch the application on it. For more information about QuickLaunch, see QuickLaunch in AWS Marketplace.

The instructions are provided by the seller and are different for each seller and product. The general steps to launch a product with a Helm fulfillment option are as follows:

To launch a product with a Helm fulfillment option

1. Follow steps 1–6 of Launch container software from AWS Marketplace, and choose a fulfillment option with a **Helm chart** delivery method.
2. In **Launch target**, choose the environment that you want to deploy on:
   - Choose **Amazon managed Kubernetes** to deploy the application in Amazon EKS. If the seller has enabled QuickLaunch, you can use it to create a new Amazon EKS cluster and launch on it.
   - Choose **Self-managed Kubernetes** to deploy the application in EKS Anywhere or on any Kubernetes cluster running in Amazon EC2 or on-premises.
3. If launching in an **Amazon managed Kubernetes** cluster:
   a. To launch on an existing cluster in Amazon EKS, under **Launch method**, choose **Launch on existing cluster** and follow the **Launch instructions**. The instructions include creating an AWS Identity and Access Management (IAM) role and launching the application. Verify that you're using Helm CLI version 3.7.1.
   b. To use QuickLaunch to create a new Amazon EKS cluster and launch on it, under **Launch method**, choose **Launch on a new EKS cluster with QuickLaunch**. Choose **Launch** to be redirected to create a stack in the AWS CloudFormation console. This stack will create an Amazon EKS cluster and deploy the application by installing the seller-provided Helm chart.
   c. On the **Quick create stack** page, in **Stack name**, provide a name for this stack.

d. Review the information in the **Parameters** tile and provide any necessary information. Review and select the acknowledgements in **Capabilities** and choose **Create stack**.

> **Note**
>
> For more information about QuickLaunch, including information about AWS CloudFormation, stacks, and the created Amazon EKS cluster, see QuickLaunch in AWS Marketplace.

4. If launching in a **Self-managed Kubernetes** cluster:

   a. Verify that you're using Helm CLI version 3.7.1.

   b. Choose **Create token** to generate a license token and IAM role. This token and role is used to communicate with AWS License Manager to validate product entitlements.

   > **Note**
   >
   > The maximum number of license tokens for an account is 10.

   c. Choose **Download as CSV** to download a .csv file with the generated token information. As with all secrets and passwords, store the .csv file in a secure location.

   d. Run the commands in **Save as Kubernetes secret** to save the license token and IAM role as a secret in your Kubernetes cluster. This secret is used when you install the Helm chart and launch the application. AWS Marketplace uses the secret to verify the entitlement for this product.

   e. Run the commands in **Launch application using token** to install the Helm chart that deploys the application to your cluster.

   f. Choose **Usage instructions** for documentation from the seller about how to configure and use the product after launching.

   g. *Optional* - Use the provided commands in **[Optional] Download artifacts** to download the product's container images and Helm charts locally.

Launching with an Amazon EKS fulfillment option

For a fulfillment option with an Add-on for Amazon EKS delivery method, use the Amazon EKS Console to deploy the software on your Amazon EKS cluster. The general steps to launch the product are as follows:

To launch a product with an Amazon EKS fulfillment option

1. After subscribing to the product, navigate to the configuration page and choose **Continue to Amazon EKS Console** to access the Amazon EKS console.
2. From the Amazon EKS console, choose the AWS Region where your cluster is deployed. Select the cluster in which you want to deploy your software.
3. Choose the **Add-ons** tab.
4. Choose **Get more add-ons**, scroll to locate the add-on that you want to deploy, and choose **Next**.
5. Select the version that you want to deploy and choose **Next**. For more information about Amazon EKS deployment, see EKS add-ons.
6. Review your selections and choose **Create**.

QuickLaunch in AWS Marketplace

If the seller has enabled QuickLaunch on a fulfillment option, you can use it to create an Amazon EKS cluster and deploy a container application to it. With QuickLaunch, you will use AWS CloudFormation to configure and create an Amazon EKS cluster and launch a container application on it. With QuickLaunch, you can launch a container application for testing purposes. To use QuickLaunch, follow the steps in Launching with a Helm fulfillment option.

To create an Amazon EKS cluster that the application can be deployed on, create a CloudFormation stack. A *stack* is a collection of AWS resources that you can manage as a single unit. All the resources in a stack are defined by the stack's CloudFormation template. In QuickLaunch, the stack's resources include the information required to create the Amazon EKS cluster and launch the application. For more information about stacks in AWS CloudFormation, see Working with stacks in the *AWS CloudFormation User Guide*.

After the cluster is created, QuickLaunch launches the application on it by installing the seller-provided Helm chart onto the cluster. QuickLaunch handles this for you as part of the stack creation that also creates the Amazon EKS cluster.

Machine learning products

AWS Marketplace has a category for machine learning products you can subscribe to through AWS Marketplace. The product category is Machine Learning. The products in this category include machine learning (ML) model packages and algorithms.

You can browse and search for hundreds of ML model packages and algorithms from a broad range of subcategories, such as computer vision, natural language processing, speech recognition, text, data, voice, image, video analysis, fraud detection, and predictive analysis.

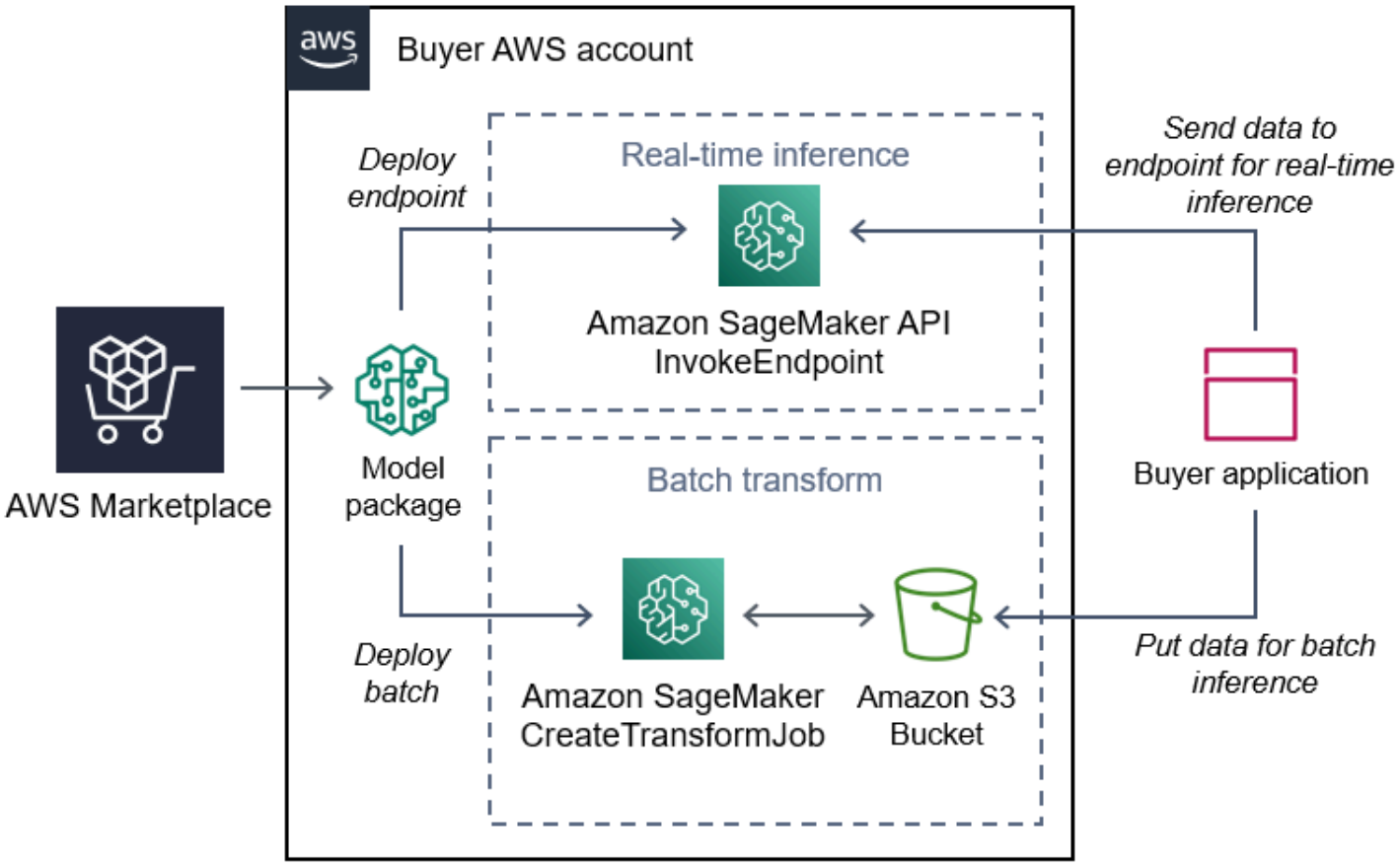
To assess the quality and suitability of a model, you can review product descriptions, usage instructions, customer reviews, sample Jupyter notebooks, pricing, and support information. You deploy models directly from the Amazon SageMaker console, through a Jupyter notebook, with the Amazon SageMaker SDK, or using the AWS Command Line Interface AWS CLI. Amazon SageMaker provides a secure environment to run your training and inference jobs by running a static scan on all marketplace products.

Amazon SageMaker model package

An **Amazon SageMaker *model package*** is a unique pretrained ML model that is identified by an Amazon Resource Name (ARN) on Amazon SageMaker. Customers use a model package to create a model in Amazon SageMaker. Then, the model can be used with hosting services to run real-time inference or with batch transform to run batch inference in Amazon SageMaker.

The following diagram shows the workflow for using model package products.

1. On AWS Marketplace, you find and subscribe to a model package product.
2. You deploy the inference component of the product in SageMaker to perform inference (or prediction) in real time or in batches.

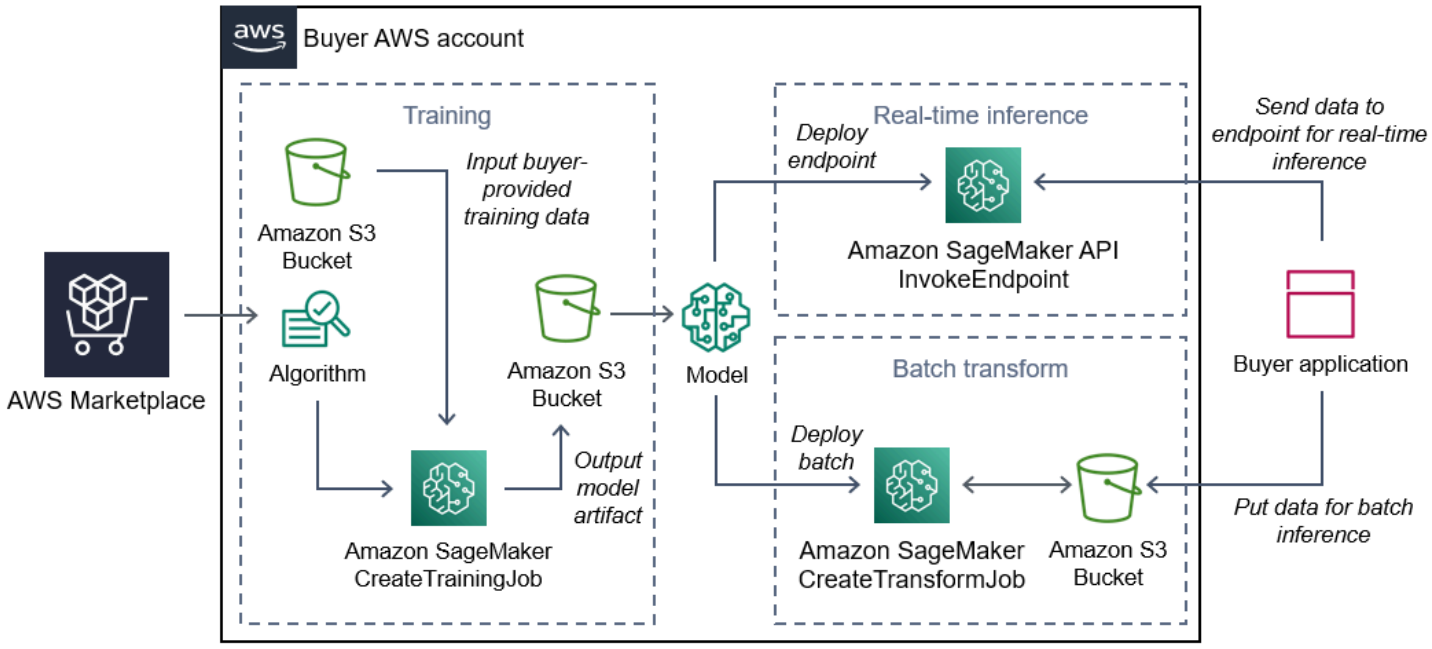


Amazon SageMaker algorithm

An **Amazon SageMaker *algorithm*** is a unique Amazon SageMaker entity that is identified by an ARN. An algorithm has two logical components: training and inference.

The following diagram shows the workflow for using algorithm products.

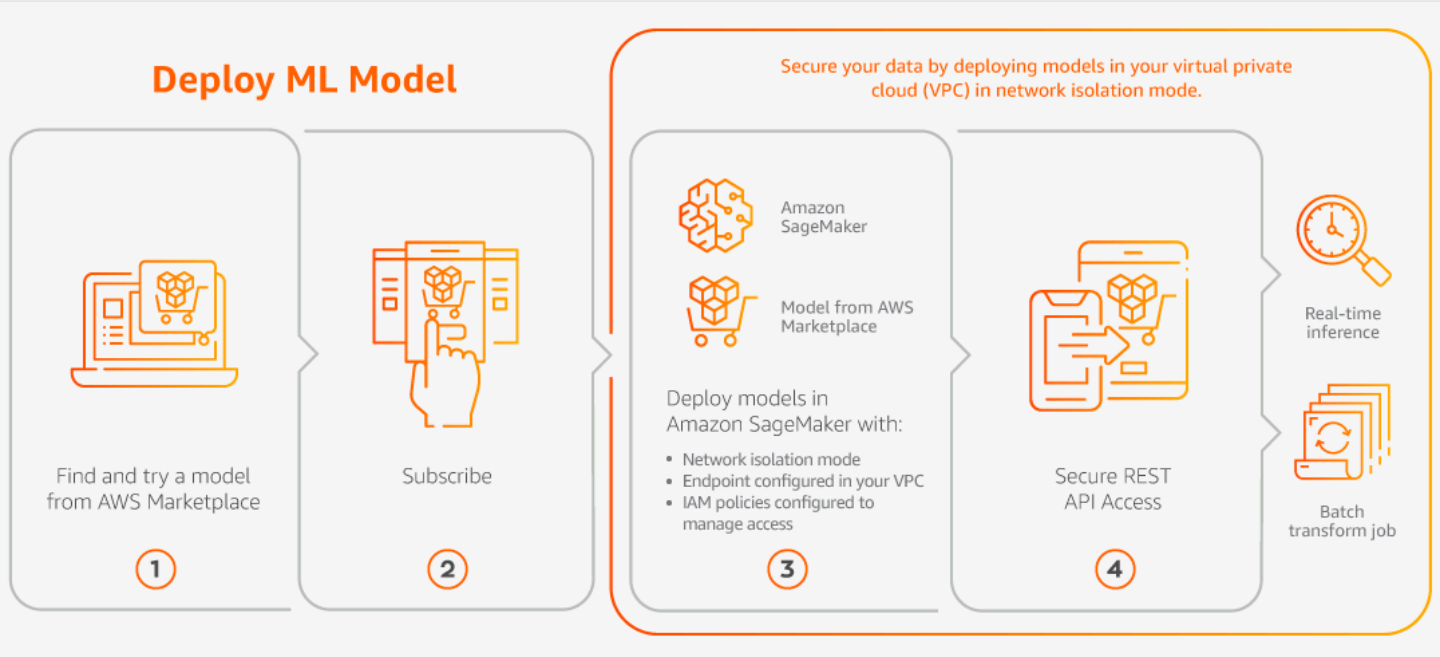
1. On AWS Marketplace, you find and subscribe to an algorithm product.
2. You use the training component of the product to create a training job or tuning job using your input dataset in Amazon SageMaker to build machine learning models.
3. When the training component of the product completes, it generates the model artifacts of the machine learning model.
4. SageMaker saves the model artifacts in your Amazon Simple Storage Service (Amazon S3) bucket.
5. In SageMaker, you can then deploy the inference component of the product using those generated model artifacts to perform inference (or prediction) in real time or in batches.



Find, subscribe, and deploy

The following diagram shows an overview of the process to find, subscribe, and deploy a machine learning product on Amazon SageMaker.

1. Find and try a model from AWS Marketplace
2. Subscribe to the ML product
3. Deploy models in Amazon SageMaker
4. Use secure REST APIs
5. Perform
   - Real-time inference
   - Batch transform job



You pay only for your usage, with no minimum fees or upfront commitments. AWS Marketplace provides a consolidated bill for algorithms and model packages, and AWS infrastructure usage charges.

The following sections explain how to find, subscribe to, and deploy an ML product.

Topics

- Finding a machine learning product
- Subscribing to a machine learning product
- Deploying a machine learning product

Finding a machine learning product

To find Amazon SageMaker model packages and algorithms

1. Sign in to the AWS Marketplace website.
2. Under **Find AWS Marketplace products that meet your needs**, use the **Categories** dropdown menu to find the subcategory under **Machine Learning** that you are interested in.
3. You can refine your search results by applying resource type, category, and pricing filters.
4. From the search results, access the product detail page.

5. Review the product description, usage instructions, customer reviews, data requirements, sample Jupyter notebooks, and pricing and support information.

Subscribing to a machine learning product

To subscribe to Amazon SageMaker model packages and algorithms

1. From the product detail page, choose **Continue to subscribe**.
2. On the procurement page, review the product pricing information and the end user license agreement (EULA).
3. Choose **Continue to subscribe**.

Deploying a machine learning product

To deploy Amazon SageMaker model packages and algorithms

1. Confirm that you have a valid subscription to the algorithm or model package by navigating to Your Marketplace Software.
2. Configure the product (for example, by selecting a specific version or deployment region) on the AWS Marketplace website.

   After you subscribe to either a model package product or algorithm product, it's added to your product list in the SageMaker console. You can also use AWS SDKs, the AWS Command Line Interface (AWS CLI), or the SageMaker console to create a fully managed REST inference endpoint or perform inference on batches of data.
3. View the Amazon SageMaker product detail page by choosing **View in Amazon SageMaker**.
4. From the Amazon SageMaker console, you can deploy the model packages and algorithms using the Amazon SageMaker console, Jupyter notebook, Amazon SageMaker CLI commands, or API operations.

For more information about deploying on Amazon SageMaker, see Getting Started.

Professional services products

AWS Marketplace includes products that are professional services from AWS Marketplace sellers. You can find these products in the *Professional Services* category when searching in AWS

Marketplace. You subscribe and purchase these products through AWS Marketplace, but you will work with the seller to set up the professional services to meet your needs.

Purchasing professional services

You can search for professional services using the *Professional Services* category in AWS Marketplace. When you find a product that interests you, request an offer from the seller. Because professional services usually involve working together, you must provide some additional information to the seller in order to complete the purchase. You can also use this as an opportunity to negotiate pricing and any other details of the service that need to be resolved. You will receive a private offer for the product. For more information about private offers, see Private offers.

To purchase a professional services product

1. Go to AWS Marketplace and sign in to your AWS account, then search and find a professional services product that you want to purchase.
2. On the product details page for the product, choose **Continue**.
3. On the **Request service** page, add the additional information that is required for the seller to create the offer, including your name, email address, company name, and any additional information that would be helpful to the seller, including business needs, timelines, and contract requirements.
4. The seller will contact you via the email address that you provided to work out the details of your offer. Once you have agreed, the seller will send you a link to the offer in AWS Marketplace. Open the link in a browser, and sign into your AWS account.
5. Review the offer details on the procurement page that you opened from the seller. Make sure that the offer is for the service you are expecting, and the price that you are expecting. Also check the terms—whether you pay a lump sum or a series of charges. If the offer is correct, continue. Otherwise, contact the seller to make changes.
6. Under **Configure contract**, choose the configuration that you would like to use for your contract. For example, if you are purchasing a support contract, there might be options for *Silver*, *Gold*, or *Platinum* contracts, with different prices.
7. Select **Create contract** to purchase the service. The seller should contact you within 2 business days with instructions for using the service.

SaaS products

For software as a service (SaaS) products, you subscribe to products through AWS Marketplace, but you access the product in the software seller's environment.

Topics

Pricing models

AWS Marketplace offers the following pricing models.

SaaS usage-based subscriptions

With SaaS usage-based subscriptions, the software seller tracks your usage and you pay only for what you use. This pay-as-you-go pricing model is similar to that of many AWS services. Billing for your usage of a SaaS product is managed through your AWS bill.

To subscribe using the SaaS usage-based subscription

1. On the product detail page, choose **View purchase options** to start the subscription process.
2. Review the subscription, and choose **Subscribe** on the subscription page.

> **Note**
>
> Some products offer a Quick Launch deployment option, which reduces the time and resources that are required to configure, deploy, and launch software. These products are identified using a Quick Launch badge. For more information, see the section called "Quick Launch".

SaaS upfront commitments

Some companies make SaaS contracts available upfront for purchase through AWS Marketplace. With this option, you can purchase discrete quantities of licenses or data ingest for these products. Then, you can bill these products, in advance, through your AWS account. For example, you might

purchase 10 user access licenses for a year, or you might purchase 10 GB of data ingest per day for a year.

When you make the purchase, you're directed to the product's website for account setup and configuration, unless Quick Launch is enabled. The usage charges then appear on your regular AWS account billing report.

> **Note**
>
> For information about the Quick Launch experience, see the section called "Quick Launch".

To subscribe with a SaaS contract

1. On the product detail page, choose **View purchase options** to start the subscription process. You can choose the quantities or units that you want, length of subscription (if multiple options are available), and automatic renewal.
2. After you have made your selections, choose **Create Contract**.
3. Choose **Set Up Your Account**, which takes you to the company's website. While your account is being configured and the payment is being verified, you will see your contract is pending on the AWS Marketplace details page for the product.

   > **Note**
   >
   > Some products offer a Quick Launch deployment option, which reduces the time and resources that are required to configure, deploy, and launch software. These products are identified using a Quick Launch badge. For more information, see the section called "Quick Launch".

After configuration is complete, a link to set up your account is available on the product page. The software appears under **Your Marketplace Software** when you're signed in to your AWS Marketplace account. You can now start using the software. If you don't complete the setup process for your account, you are prompted to do so when you revisit that product on AWS Marketplace.

Access the software subscription from the software company's website using the account you created on their website. You can also find website links for software subscriptions that you

purchased through AWS Marketplace under **Your Marketplace Software** when you're signed in to your AWS Marketplace account.

SaaS free trials

Some vendors offer free trials for their SaaS products through AWS Marketplace for evaluation purposes. You can search through SaaS products on AWS Marketplace and filter results to only show those with free trials. Search results indicate which products offer free trials. All free trial products display the **Free trial** badge next to the product logo. On the product procurement page, you can find the duration of the free trial period and how much free software usage is included in the trial.

During the free trial, or after the free trial expires, you can make a purchase decision by negotiating a private offer or subscribing to a public offer. SaaS free trials won't automatically convert into paid agreements. If you no longer want the free trial, you can let the free trial expire.

You can view your subscriptions by selecting **Manage subscriptions** from the AWS Marketplace console.

> **Note**
>
> Each AWS account is only eligible for 1 free trial per product.

Subscribing to a SaaS contract free trial offer

To subscribe to a SaaS contract free trial offer

1. Sign in to the AWS Marketplace console, and choose **Discover products** from the AWS Marketplace menu.
2. In the **Refine results** panel, go to **Free trial** and select **Free trial**.
3. For **Delivery methods**, select **SaaS**.
4. For **Pricing model**, select **Upfront Commitment** to view all products that offer free trials. All eligible products display a **Free trial** badge.
5. Select the SaaS product that you want.
6. Choose **Try for free** from the product detail page.
7. For **Offer type**, select a **Free trial** option.
8. For **Purchase**, choose **Create contract** and then **Accept contract**.

9. Choose **Set up your account** to complete your registration and start using your software.

Subscribing to a SaaS subscription free trial offer

To subscribe to a SaaS subscription free trial offer

1. Sign in to the AWS Marketplace console, and choose **Discover products** from the AWS Marketplace menu.
2. In the **Refine results** panel, go to **Free trial** and select **Free trial**.
3. For **Delivery methods**, select **SaaS**.
4. For **Pricing model**, select **Usage Based** to view all products that offer free trials. All eligible products display a **Free trial** badge.
5. Select the SaaS product that you want.
6. Choose **Try for free** from the product detail page.
7. For **Offer type**, select a **Free trial** option.
8. For **Purchase**, choose **Subscribe**.

Quick Launch

Quick Launch is an AWS Marketplace deployment option that's available for SaaS products that have Quick Launch enabled. It reduces the time, resources, and steps required to configure, deploy, and launch your software. For products that offer this feature, you can either choose to use Quick Launch or manually configure your resources.

To find, subscribe, and launch a SaaS product using the Quick Launch experience

1. Navigate to the AWS Marketplace search page.
2. Browse AWS Marketplace, and find the product that contains the software that you want to launch. Products that provide the Quick Launch experience have a **Quick Launch** badge in their product description.

> **Tip**
>
> To find products with the Quick Launch experience enabled, use the **SaaS** and **CloudFormation template** filters in the **Refine results** pane.

3. After you subscribe to the product, navigate to the **Configure and launch** page by choosing the **Set Up Your Account** button.
4. On the **Configure and launch** page in **Step 1: Make sure you have required AWS permissions**, make sure that you have the permissions necessary to use the Quick Launch experience. Contact your AWS administrator to request the permissions.

   To use the full Quick Launch experience, you must have the following permissions:

   - `CreateServiceLinkedRole` – Allows AWS Marketplace to create the `AWSServiceRoleForMarketplaceDeployment` service-linked role. This service-linked role allows AWS Marketplace to manage deployment-related parameters, which are stored as secrets in AWS Secrets Manager, on your behalf.
   - `DescribeSecrets` – Allows AWS Marketplace to obtain information about deployment parameters passed by sellers.
   - `GetRole` – Allows AWS Marketplace to determine if the service-linked role has been created in the account.
   - `ListSecrets` – Allows AWS Marketplace to obtain the status of the deployment parameters.
   - `ListRegions` – Allows AWS Marketplace to obtain AWS Regions that are opted in for the current account.
   - `ReplicateSecrets` – Allows AWS Marketplace to start the replication of secrets to the selected Region where you will deploy the software.
5. For **Step 2: Log into an existing or new vendor account**, choose the **Log in or create an account** button. The seller's site opens in a new tab, where you can either log in or create a new account. When you're done, return to the **Configure and launch** page.
6. For **Step 3: Configure your software and AWS integration**, choose how you want to configure the product:

   - AWS CloudFormation – Choose the **Launch template** button to deploy a predefined CloudFormation template to configure your product. Use CloudFormation to review the template parameters and complete any additional required fields. When you're done, return to the **Configure and launch** page to launch your software.
   - Manual – Use the instructions provided by the seller to configure your software.
7. For **Step 4: Launch your software**, choose the **Launch software** button to launch your software.

Data products

You can use AWS Marketplace to find and subscribe to data products available through AWS Data Exchange. For more information, see Subscribing to Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Paying for products

At the beginning of the month, you receive a bill from Amazon Web Services (AWS) for your AWS Marketplace charges. For software products, the bill includes a calculation of the hourly fee for the software multiplied by the number of hours any Amazon Machine Image (AMI) instance with this software runs. You also receive a bill for usage of AWS infrastructure services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), and for bandwidth.

If your AWS account is based in Europe, the Middle East, and Africa (EMEA), excluding Turkey and South Africa, and your purchase is from an EMEA-eligible seller, you receive a bill from Amazon Web Services EMEA SARL (AWS Europe). If your AWS account is based in Australia, you receive a bill from Amazon Web Services Australia Pty Ltd (AWS Australia). If your AWS account is based in Japan, you receive a bill from Amazon Web Services Japan G.K (AWS Japan). Otherwise, you receive a bill from AWS Inc.

Note

For AMI annual and contract purchases, the invoice for the subscription fees happens at the time of subscription, rather than in the consolidated monthly bill. AMI annual purchases generate a single invoice for the entire agreement that covers all the instance types purchased during the subscription. Flexible payments on contracts are invoiced at the time of the scheduled payment. For contracts that have usage components (such as a pay-as-you-go model), the usage appears in your consolidated monthly bill.

AWS Marketplace products using complex topologies may incur charges for clusters of AMIs and other AWS infrastructure services launched by the provided AWS CloudFormation template.

For example, suppose that you run software for 720 hours on an EC2 small instance type. The seller's fee for software usage is $0.12 per hour and the EC2 charges are $0.085 per hour. At the end of the month, you are billed $147.60.

For more information about subscribing to data products, see Subscribing to data products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

For more information about paying your AWS bill, see the AWS Billing User Guide.

For more information about managing your payments in Amazon Web Services EMEA SARL (AWS Europe), see Managing your payments in AWS Europe in the *AWS Billing User Guide*.

Topics

Purchase orders

When you use purchase orders in AWS Marketplace and the AWS Billing console, you receive invoices from AWS that include the customer-defined purchase order number. This approach simplifies payment processing and cost allocation. In AWS Marketplace, out-of-cycle invoices include purchases that are billed either immediately or according to a defined payment scheduled in a private offer. Generally, pay-as-you-go charges appear on a consolidated AWS Marketplace monthly usage invoice.

Using purchase orders for AWS Marketplace transactions

You can add a purchase order at the time of transaction, which will apply to all subsequent out-of-cycle invoices related to that transaction.

The following products support purchase orders:

- Software as a service (SaaS) contracts
- Professional service products
- Server products (including AMI instances, containers, AWS CloudFormation templates, and Helm charts with an annual or contract pricing model

> **Note**
>
> Purchase order support for the annual pricing model is only available for private offers with a flexible payment schedule.

Purchase orders for the annual pricing model are only supported for private offers with a flexible payment schedule. The purchase order that you specify doesn't apply to consolidated AWS Marketplace monthly invoices for pay-as-you-go charges.

> **Note**
>
> To use purchase orders in AWS Marketplace, the management account in your AWS organization must enable the AWS Billing integration. This one-time setup task creates a service-linked role, which allows accounts in your organization with permission to subscribe to use purchase orders. If you don't enable the integration, accounts in your organization can't add a purchase order during procurement. For more information about the integration, see Creating a service-linked role for AWS Marketplace.

To specify a purchase order in AWS Marketplace

1. Find and prepare to purchase a supported product from AWS Marketplace.
2. During the purchase process, on the **Configure your software subscription** page (for SaaS), for **Purchase order**, choose **Add purchase order number**.
3. Enter your purchase order number in the **Purchase order number** field.

   Your purchase order number is the number or text that you use to track your purchase order in your system. It's usually issued by an internal system or process. It can be up to 200 characters in length.

For details about a purchase order, including purchase orders provided during AWS Marketplace transactions, use the purchase orders dashboard in the AWS Billing console.

Using blanket usage purchase orders

To separate AWS Marketplace charges from other purchase orders, you can create a purchase order with an AWS Marketplace blanket usage line item in the AWS Billing console. AWS Marketplace invoice transactions will include the blanket usage purchase order that you specify if certain criteria and parameters match (for example, billing entities). An exception is out-of-cycle bills that have specified an AWS Marketplace transaction purchase order. For more information, see Managing your purchase orders in the *AWS Billing and Cost Management User Guide*.

Troubleshooting purchase orders

The information in the following table can help you troubleshoot issues with purchase orders, or understand what happens in different scenarios.

Scenario	Details
Insufficient permissions	The note displays near the **Purchase order entry** field if you don't have the `aws-marketplace:Subscribe` permission to subscribe. The management account must also enable the AWS Billing integration. For information about enabling the integration, see Creating a service-linked role for AWS Marketplace.
Purchase order does not exist	AWS Marketplace creates a new purchase order for you. The new purchase order has default information, with no contact information.
Missing purchase order notifications	Purchase orders without contact information (including the purchase orders created by AWS Marketplace) do not receive email notifications. You can add contact information to a purchase order in the Purchase Orders dashboard in the Billing and Cost Management console.

Scenario	Details
Incorrect purchase order number added	If you enter an incorrect purchase order number and need to update it, contact AWS Support to update the purchase order number.
Subscribing account moves to a different organization	For purchase orders to work in the new organization, the integration must be completed in the new organization. If integrati on has been completed, and purchase order support is working in the new organization, then when the subscribing account moves between organizations, new invoices show the purchase order number in the new organizat ion (and a new purchase order is created, if necessary).
Purchase order option not available when checking out	The AWS Billing integration is only available for SaaS contracts, professional service products, and server products with contract pricing, and server products with annual pricing for private offers with a flexible payment schedule.
Contracts with pay-as-you-go	The invoice for the contract shows the purchase order number, but the invoice for consumption (pay as you go) does not show the purchase order number. The pay-as-you-go model does not support adding purchase order numbers. Consider adding a purchase order with an AWS Marketplace blanket usage line item in the AWS Billing console.

Scenario	Details
Suspended purchase order	When a purchase order number is provided, and the purchase order is marked as suspended in the Purchase Orders dashboard in the Billing and Cost Management console, the new line item is added to the purchase order, but the invoice does not include the purchase order. The billing admin for the AWS account needs to make the purchase order active, and contact AWS Support to regenerat e the invoice with the active purchase order.
Expired purchase order	When a purchase order number is provided, and the purchase order is expired, the new line item is created and the purchase order is marked as active. The line item's end date is used as the new purchase order expiration date.
Balance tracking	Balance tracking is not enabled for AWS Marketplace line items.
Procurement system integration	The purchase order provided by an integrated procurement system is shown on invoices.
Flexible payment schedule - initial purchase	A contract that has specific dates for invoicing (flexible payment schedule) generates an initial line item in the purchase order for zero dollars. Additional line items with applicable prices are created for each invoice.
Flexible payment schedule - multiple purchase orders	If you need your individual payments for a flexible payment schedule to show up with different purchase orders, contact AWS Support to change the purchase order number on future invoices.

Information about refunds

Customers can request different types of refunds for AWS Marketplace products. For AWS Marketplace products sold by AWS, refer to the refund policy page and then submit the contact support form using the AWS Support Center Console. If the product is sold by a third-party, review the refund policies on the product detail page. Software charges for AWS Marketplace subscriptions are paid to the seller of the product, and refunds must be requested from the seller directly. Each AWS Marketplace seller is required to include a refund policy on their AWS Marketplace page.

For more information about refunds related to your AWS Marketplace purchases, see the following topics in the *AWS Marketplace Seller Guide*:

- Refunds
- Product pricing

> **Note**
>
> For all refunds related to private offers, contact the seller.

Cancel your product subscription

You can cancel your product subscription or auto-renewal in AWS Marketplace. The following steps provide instruction for software as a service (SaaS), machine learning (ML), and Amazon Machine Image (AMI) products in AWS Marketplace.

Topics

- Cancel your SaaS subscription
- Cancel your machine learning subscription
- Cancel your AMI subscription
- Cancel auto-renewal for your SaaS contract subscription

Cancel your SaaS subscription

1. Sign in to the AWS Management Console and open the AWS Marketplace console.

2. Go to the **Manage subscriptions** page.
3. For the delivery method, choose **SaaS** from the dropdown list.
4. Select the subscription for the product that you want to cancel.
5. Choose **Cancel subscription**.

Cancel your machine learning subscription

Before you cancel your machine learning subscription, take the following actions:

- For ML algorithms – Sign in to the AWS Management Console and open the Amazon SageMaker console. Terminate any running training jobs for your algorithm. If you created a model package from your algorithm, you can't launch a real-time endpoint or create a batch inference job after your machine learning subscription is canceled.
- For ML model packages or models created from your algorithms – Sign in to the AWS Management Console and open the Amazon SageMaker console. Terminate any running real-time endpoints for your models or terminate any running batch inference jobs.

> **Note**
>
> Existing jobs and endpoints that aren't terminated will continue to run and will be billed until they are terminated.

To cancel a machine learning subscription

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Go to the **My Subscriptions** page.
3. Select the subscription for the product that you want to cancel.
4. Choose **Cancel subscription**. After canceling your subscription, you can't launch your algorithm or model.

Cancel your AMI subscription

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Go to the **Manage subscriptions** page.

3. For the delivery method, choose **Amazon Machine Image** from the dropdown list.
4. Select the subscription for the product that you want to cancel.
5. From the **Actions** dropdown list, choose **Cancel subscription**.
6. Read the information provided to **Acknowledge that running instances are charged to your account** and select the check box. Choose **Yes, cancel subscription**.
7. Open **Manage in AWS Console** in a new tab.
8. Terminate the running instance in the Amazon EC2 console. If you have multiple instances running, you must terminate all of them. Also, you must delete AWS CloudFormation stacks, if applicable.
9. Return to the **Manage subscriptions** tab and choose **Yes, Cancel subscription**. After canceling your subscription, you lose access to the software and will no longer be billed for it.

Cancel auto-renewal for your SaaS contract subscription

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Go to the **Product detail** page.
3. Choose **Continue** to get to the ordering page.
4. Choose the **Modify renewal** tab and then choose **Cancel renewal**.

Payment methods

When you first created your AWS account, you set the payment method for that account. You can manage your payment methods in the AWS Billing and Cost Management console. For instructions, see Managing your payments in the *AWS Billing User Guide*.

Payment errors

If an error occurs while processing your payment through your payer account, update your payment method and try again. Errors can occur because:

- The payment method is missing, invalid, or unsupported.
- The payment was declined.
- Your Amazon Internet Services Private Limited (AISPL) account limits the use of debit or credit cards for new purchases with a contract pricing model. If you have an AISPL account, contact

AWS Customer Service to update your default payment method. For more details, see Restriction on credit and debit card purchases for AISPL customers using AWS Marketplace at the AWS Marketplace Blog website.

- Your private offer includes a payment schedule. However, your default payment method isn't set to invoicing terms.

Updated payment methods can take up to 7 days to become available for new purchases. For help with troubleshooting, contact AWS Support.

Supported currencies

The following lists include all existing supported currencies for AWS, Amazon Web Services EMEA SARL, Amazon Web Services Australia, and Amazon Web Services Japan G.K.

> **Note**
>
> The Indian rupee (INR) is not a supported currency because Amazon Internet Services Private Limited (AISPL) isn't currently supported on AWS Marketplace. For more information, see What are the differences between AWS accounts and AISPL accounts.

The supported currencies for Amazon Web Services are as follows:

- Australian dollar (AUD)
- British pound (GBP)
- Canadian dollar (CAD)
- Danish krone (DKK)
- Euro (EUR)
- Hong Kong dollar (HKD)
- Japanese yen (JPY)
- New Zealand dollar (NZD)
- Norwegian krone (NOK)
- Singapore dollar (SGD)
- South African rand (ZAR)

- Swedish krona (SEK)
- Swiss franc (CHF)
- US dollar (USD)

The supported currencies for Amazon Web Services EMEA SARL are as follows:

- British pound (GBP)
- Danish krone (DKK)
- Euro (EUR)
- Norwegian krone (NOK)
- South African rand (ZAR)
- Swedish krona (SEK)
- Swiss franc (CHF)
- US dollar (USD)

The supported currencies for Amazon Web Services Australia are as follows:

- Australian Dollar (AUD)
- US Dollar (USD)

The supported currencies for Amazon Web Services Japan G.K. are as follows:

- Japanese Yen (JPY)
- US Dollar (USD)

Changing your preferred currency

Your AWS Marketplace purchases are displayed in the currency that you specified for your AWS account. You can change your preferred currency for your account in the AWS Billing and Cost Management console. For instructions, see Changing which currency you use to pay your bill in the *AWS Billing User Guide*.

> **Note**
>
> Changing your preferred currency changes your remittance instructions. To view updated remittance instructions, see your AWS Marketplace invoice or view the **Account Settings** page in the AWS Billing and Cost Management console.

Updating remittance instructions

Customers with AWS accounts based in Europe, the Middle East, and Africa (EMEA), excluding Turkey and South Africa, who have purchased software products from EMEA-eligible sellers receive a bill from Amazon Web Services EMEA SARL. Amazon Web Services EMEA SARL (AWS Europe) invoices have different remittance instructions from AWS, Inc. You can find remittance information on your bills when signed in to the AWS Billing and Cost Management console. The bank accounts listed under the remittance information portion of the invoice are different from AWS Cloud services purchases through Amazon Web Services EMEA SARL. Amazon Web Services EMEA SARL uses Amazon Payments Europe, S.C.A., a licensed electronic money institution in Luxembourg, as its payment processor for AWS Marketplace invoices. All invoices must be settled in full. Any payments that don't cover the full invoice amount will be refunded to your bank account.

The following table outlines the transaction types, the transacting entity, and the corresponding remittance instructions (**Account Name** listed under **Electronic funds transfer details** on the invoice).

Type of transaction	Transacting entity	Remittance instructions
AWS Cloud services purchases	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
Eligible AWS Marketplace seller	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
Ineligible AWS Marketplace seller	AWS Inc.	AWS

To request a bank letter for the remittance instructions, select **Billing or account support** and create an **Account and billing support** case at Contact AWS or send an email message to <awslux-receivables-support@email.amazon.com>.

For more information about how to change your currency preference to a supported currency, see Changing which currency you use to pay your bill in the *AWS Billing User Guide*.

Amazon Web Services EMEA SARL accepts payments by electronic funds transfer, by MasterCard, VISA, and American Express credit cards. Diner's Club or Discover credit cards are not accepted.

For more information, see AWS Marketplace Buyer Tax Help.

Cost allocation tagging

AWS Marketplace supports cost allocation tagging for software products that you purchase. You can use activated cost allocation tags to identify and track AWS Marketplace resource usage through AWS Cost Explorer, AWS Cost and Usage Reports, AWS Budgets, or other cloud cost analysis tools. To make it easier for you to categorize and track your AWS Marketplace costs, you can use cost allocation tags to organize your resource costs on your cost allocation report.

Cost allocation tags in AWS Marketplace come from the following two sources:

- Amazon Machine Image (AMI) software product costs that are associated with an Amazon Elastic Compute Cloud (Amazon EC2) instance with tags inherit those same tags. You can activate these tags as cost allocated tags in the AWS Billing and Cost Management console for an account. For more information about using cost allocation tags with AMI products, see Cost allocation tagging in AMI products.
- AMI, container, and software as a service (SaaS) products may have vendor-provided tags. For example, a SaaS product that bills by the number of users could use a tag to identify the usage by department. For more information about using these tags, see Vendor-metered tags.

Cost allocation tagging only tracks costs from the time when the tags were activated in the Billing and Cost Management console. Only AWS account owners, AWS Organizations management account owners, and users with the appropriate permissions can access the Billing and Cost Management console for an account. Regardless of whether you use cost allocation tagging, there's no change to how much you're billed. Whether you use cost allocation tags has no impact on the functionality of your AWS Marketplace software products.

For subscriptions from EMEA-eligible sellers, the Cost and Usage Report includes a column for the AWS Contracting Party (Amazon Web Services EMEA SARL).

Vendor-metered tags

AWS Marketplace products with vendor metering (including AMI, container, and SaaS products) might have tags provided by the software vendor as an added service for their customers. These tags are cost-allocation tags that help you understand your AWS Marketplace resource usage across vendor-provided metrics. You can use these tags to identify and track AWS Marketplace resource usage through AWS Cost Explorer Service, AWS Cost and Usage Report, AWS Budgets, or other cloud cost analysis tools.

The tags appear in your AWS Billing console after you start using the AWS Marketplace product and the vendor sends metering records to AWS Marketplace. If you're using a product based on an upfront commitment in a contract, you won't receive metering usage for the product. As a result, you won't have the vendor-metered tags in your AWS Billing console. If you're managing a linked account, you must have both the `ModifyBilling` and `ViewBilling` permissions to view and activate tags in AWS Billing. For more information, see AWS Billing actions policies in the *AWS Billing User Guide*.

> **Note**
>
> Activating vendor-metered tags could increase your cost and usage report's size. Your cost and usage report is stored in Amazon S3. Therefore, your Amazon S3 costs could increase also.

To activate vendor-metered tags for all eligible AWS Marketplace products

1. Sign in to the AWS Management Console and open the AWS Billing console. Then choose **Cost allocation tags** from the left navigation pane.
2. Choose the **AWS-generated cost allocation tags** tab.
3. Search for `aws:marketplace:isv:` to find tags for all products that support vendor-metered tagging.
4. Select the check boxes for all tags, and then choose **Activate**. Your vendor-metered tags will go into effect within 24 hours.

Related topics

For more information, see the following topics:

- Using Cost Allocation Tags in the *AWS Billing User Guide*
- Activating the AWS-Generated Cost Allocation Tags in the *AWS Billing User Guide*

Private marketplaces

A private marketplace controls which products users in your AWS account, such as business users and engineering teams, can procure from AWS Marketplace. It is built on top of AWS Marketplace, and enables your administrators to create and customize curated digital catalogs of approved independent software vendors (ISVs) and products that conform to their in-house policies. Users in your AWS account can find, buy, and deploy approved products from your private marketplace, and ensure that all available products comply with your organization's policies and standards.

A private marketplace provides you with a broad catalog of products available in AWS Marketplace, along with fine-grained control of those products. With AWS Organizations, you can centralize management of all of your accounts, group your accounts into organizational units (OUs), and attach different access policies to each OU. You can create multiple private marketplace experiences that are associated with your entire organization, one or more OUs, or one or more accounts in your organization, each with its own set of approved products. Your AWS administrators can also apply company branding to each private marketplace experience with your company or team's logo, messaging, and color scheme.

This section describes using private marketplace as a buyer. For information about managing private marketplaces as an administrator, see Creating and managing a private marketplace.

Notes

- You can add private products that have been shared with you (through a private offer) to a private marketplace. For more information, see Subscribing to a private product in a private marketplace.
- In a private marketplace, customers are automatically entitled to any products whose EULAs are governed by the AWS Customer Agreement or other agreement with AWS governing use of AWS services. Customers are already entitled to these products by default; therefore, they are not included in the list of products that you approved within your private marketplace. Customers can use Service Catalog to manage the deployment of these products.

Viewing product detail pages

Users can only subscribe to products you have allowed in the private marketplace that governs the account. They can browse and see the detail page for any product, but subscription is enabled only for products you have added to your private marketplace. If a product is not currently in your private marketplace, the user sees a red banner at the top of the page, noting that the product is not approved for procurement in AWS Marketplace.

If software requests are enabled, users can choose **Create request** on the product details page. When users choose **Create request**, they submit a request to the administrator to make the product available on your private marketplace. For more information about this feature, see Managing user requests.

Subscribing to a product in a private marketplace

To subscribe to a product in your private marketplace as a user, navigate to the product's details page and choose **Continue**. This redirects you to the product's subscription page. On the subscription page, you can make your configuration selections, and then choose **Subscribe**.

If the product is not approved in your private marketplace, **Subscribe** isn't available. A red banner at the top of the page indicates that the product is not currently approved for procurement. If software requests are enabled, you can choose **Create request** to submit a request to your administrator requesting that the product be added to your private marketplace.

Subscribing to a private product in a private marketplace

Some products are not publicly available to browse in AWS Marketplace. These products can only be seen when you are given a private offer from the seller. However, you can only subscribe if your private marketplace administrator first adds the product to your private marketplace. Because of this, the private offer must be extended to both your AWS account and the account that includes your organization's private marketplace administrator. After the private offer has been extended to both the user and the administrator, the private marketplace administrator can add the product to your private marketplace. After the product has been approved, you can subscribe to the product like any other private offer.

Requesting a product be added to your private marketplace

As a user, you can request that your administrator add a product that is not in your private marketplace. To make a request, navigate to the product's details page, choose **Create request**, enter a request to your administrator that the product be added to your private marketplace, and then submit your request. To track your request status, on the left dropdown menu, choose **Your Private Marketplace Requests**.

Creating and managing a private marketplace

To create and manage a private marketplace, you must be signed into the management account or the delegated administrator account for private marketplace. You must also have the AWS Identity and Access Management (IAM) permissions in the AWSPrivateMarketplaceAdminFullAccess IAM policy. For more information about applying this policy to users, groups, and roles, see the section called “Creating a private marketplace administrator”.

> **Note**
>
> If you're a current private marketplace customer without the AWS Organizations integration for private marketplace, you can create and manage a private marketplace from any account in your organization that has the AWSPrivateMarketplaceAdminFullAccess IAM policy.

This section includes tasks that you can complete as a private marketplace administrator through the AWS Marketplace website. You can also manage private marketplaces using the AWS Marketplace Catalog API. For more information, see Working with a private marketplace in the *AWS Marketplace Catalog API Reference*.

Getting started with private marketplace

To get started with private marketplace, ensure you're signed into your AWS management account, navigate to Private Marketplace, and then enable the following prerequisites:

- **Trusted access** – You must enable trusted access for AWS Organizations, which allows the management account of an organization to provide or revoke access for their AWS Organizations data for an AWS service. Enabling trusted access is critical for private marketplace to integrate

with AWS Organizations and designate private marketplace as a trusted service in your organization.

- **Service-linked role** – You must enable the private marketplace service-linked role, which resides in the management account and includes all the permissions that private marketplace requires to describe AWS Organizations and update private marketplace resources on your behalf. For more information on the service-linked role, see Using roles to configure Private Marketplace in AWS Marketplace.

> **Note**
>
> Current private marketplace customers can enable settings for your private marketplace by navigating to the **Private Marketplace** administrator's page and choosing **Settings**. By enabling trusted access for AWS Organizations and creating a service-linked role, you can utilize features, such as associating OUs to private marketplace experiences and registering a delegated administrator. When enabled, only the management account and delegated administrator account can create and manage marketplace experiences, with existing resources transferred to the management account and shared only with the delegated administrator. Disabling trusted access will remove private marketplace governance for your organization. There are no account groups displayed in your private marketplace. To view your organization's governance at different levels, use the **Organization structure** page. For questions or support, contact us.

Managing private marketplace

You can manage your private marketplace from the **Private Marketplace** administrator's page under **Settings** in the left pane. The management account administrator and delegated administrators can use this page to view private marketplace details, including the default private marketplace and number of live experiences.

Management account administrators can also use this page to manage the following settings.

Delegated administrators

The management account administrator can delegate private marketplace administrative permissions to a designated member account known as delegated administrator. To register an account as a delegated administrator for the private marketplace, the management account

administrator must ensure trusted access and the service-linked role are enabled, choose **Register a new administrator**, provide the 12-digit AWS account number, and choose **Submit**.

Management accounts and delegated administrator accounts can perform private marketplace administrative tasks, such as creating experiences, updating branding settings, associating or disassociating audiences, adding or removing products, and approving or declining pending requests.

Trusted access and service-linked role

The management account administrator can enable the following features for your private marketplace.

> **Note**
>
> Current private marketplace customers can enable settings for your private marketplace by navigating to the **Private Marketplace** administrator's page and choosing **Settings**. By enabling trusted access for AWS Organizations and creating a service-linked role, you can utilize features, such as associating OUs to private marketplace experiences and registering a delegated administrator. When enabled, only the management account and delegated administrator account can create and manage marketplace experiences, with existing resources transferred to the management account and shared only with the delegated administrator. Disabling trusted access will remove private marketplace governance for your organization. There are no account groups displayed in your private marketplace. To view your organization's governance at different levels, use the **Organization structure** page. For questions or support, contact us.

- **Trusted access** – You must enable trusted access for AWS Organizations, which allows the management account of an organization to provide or revoke access for their AWS Organizations data for an AWS service. Enabling trusted access is critical for private marketplace to integrate with AWS Organizations and designate private marketplace as a trusted service in your organization.
- **Service-linked role** – You must enable the private marketplace service-linked role, which resides in the management account and includes all the permissions that private marketplace requires to describe AWS Organizations and update private marketplace resources on your behalf. For more information on the service-linked role, see Using roles to configure Private Marketplace in AWS Marketplace.

Creating a private marketplace experience

Your private marketplace is made up of one or more private marketplace experiences. An experience can be associated with your entire organization, one or more OUs, or one or more accounts in your organization. If your AWS account is not a member of an organization, then you have one private marketplace experience associated with one account. To create your private marketplace, navigate to Private Marketplace, select the **Experiences** page on the left, and choose **Create experience**.

> **Note**
>
> To use private marketplace with AWS Organizations, you need to enable all features for the organization. For more information, see Enabling all features in your organization in the *AWS Organizations User Guide*.
> If your AWS account is not a member of an organization, you do not need any prerequisite steps to use private marketplace.

Your private marketplace experience is created with no approved products, no branding elements, and is associated with no accounts in your organization. It's not live by default. The following topics describe how to work with your private marketplace experience.

Adding products to your private marketplace experience

To add products to a private marketplace experience

1. From the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane. Then, on the **Products** tab, choose **All AWS Marketplace products**. You can search by product name or seller name.
2. Select the check box next to each product to add to your private marketplace and then choose **Add to Private Marketplace**.

> **Note**
>
> You can also add a product directly from the product details page by choosing the **Add to Private Marketplace** button on the red banner. If the red banner is not on the product's detail page, the product is already in your private marketplace.

You can also add multiple products to multiple experiences at one time by choosing **Bulk add/ remove products** from the left navigation pane.

Verifying products in your private marketplace experience

To verify a product is approved in your private marketplace experience

1. From the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane.
2. Choose **Approved products**. All approved products display in the approved list.

> **Note**
>
> If you are using an account that has been associated with the experience you are editing, and the experience is enabled, then you can also view the products directly in the AWS Marketplace console (https://console.aws.amazon.com/marketplace). All products in any search results show an *approved for procurement* badge if they are part of your private marketplace.

Customizing your private marketplace experience

Experiences are subsets of products and associated branding that can have one or more associated audiences. A single private marketplace experience can govern the entire organization if the experience is associated to the organization or govern one or more accounts or organizational units in your organization.

You can manage your experience settings from the **Private Marketplace** administrator's page under **Experiences** in the left pane. Use this page to view and manage all your active and archived experiences and create new experiences for your private marketplace. For each experience, you can add a logo, add a title, and customize the user interface to use your organization’s color scheme.

Managing audiences

An audience is an organization or a group of organizational units (OUs) or accounts that you can associate with a private marketplace experience. You can create an audience from the **Private Marketplace** administrator's page under **Experiences** in the left pane.

You can associate one or more audiences to an experience. When you associate or disassociate an audience, it may change the governing experience of child OUs and accounts. Use the **Organization structure** page to see the accounts and OUs affected by the association. If you disable trusted access, your audiences will be disassociated and all governance will be removed.

> **Note**
>
> You can view your AWS Organizations hierarchy and manage governance for your organization from private marketplace. To govern your private marketplace at an organizational unit level and register delegated administrators, enable trusted access and the service-linked role from the **Settings** page. For questions or support, contact us.

Configuring your private marketplace

After you are satisfied with the experience's product list, the marketplace's branding settings, and the associated account groups, then you can make your private marketplace live. From the **AWS Private Marketplace** administrator's page, select **Experience** in the left navigation pane, then select the experience you want to enable. On the **Settings** tab, you can change the private marketplace status between **Live** (enabled) and **Not live** (disabled).

You can also choose to allow users to submit software requests with **Software requests**. If software requests are **On** (enabled), end users can choose **Create request** on the product details page to submit a request to the administrator to make the product available on your private marketplace. Software requests are enabled by default, and the setting can only be modified while the private marketplace is enabled.

When your private marketplace is live, end users can buy only the products that you have approved. When your private marketplace is disabled, you retain the list of products. However, disabling a private marketplace removes the restriction from users in your AWS Organizations organization. As a result, they can subscribe to any products in the public AWS Marketplace.

Making a private marketplace live does not disrupt active Amazon Machine Images (AMIs) running on Amazon Elastic Compute Cloud (Amazon EC2) instances. As a best practice, ensure that all AWS Marketplace products currently in use across your organization are included in your private marketplace. It's also a best practice to have a plan in place to discontinue use of unapproved products before making the private marketplace live. After the private marketplace is live, all new subscriptions or renewals are governed by the products approved in the private marketplace catalog.

Working with private products

Some products are not publicly available to browse in AWS Marketplace. These products can only be seen when you are given a private offer from the seller. The private offer from the seller includes a link to the product. You can add the product to the private marketplace from the banner at the top of the page.

> **Note**
>
> If you want to subscribe to a private product from a different account in your organization, the seller must include both your AWS account (to add the product to the private marketplace) and the user's account (to subscribe to the product) in the private offer.

To remove a private product from your private marketplace, you must contact AWS Marketplace Support.

Managing user requests

You can allow users to submit requests for products to be added to their private marketplace catalog with the software request feature. To do so, navigate to the administrator's page for your private marketplace, select **Experiences** in the left navigation pane, and choose the experience you want to manage. From the **Products** tab, choose **Pending requests**. From here you can review requests your users have made for products to be added to their private marketplace catalog.

You can add any number of requested products from this page by first selecting the check box next to the name of each requested product, and then choosing **Add to Private Marketplace**. Similarly, you can also decline one or more selected requests by choosing **Decline**. To view more information about a product (or its software request), choose **View details** in the **Details** column for that request.

When you decline a product request, you can add a reason and prevent future requests (block) for this product. Blocking a product won't prevent you from adding the product to your private marketplace, but it does prevent your users from requesting the product.

Archiving and reactivating a private marketplace experience

You can remove a private marketplace experience by archiving it. Archived experiences can’t be updated or used to govern accounts in your organization. If you have audiences associated with

an archived experience, you can associate them with a different experience. If you decide to use the experience at a later time, you can always reactivate it. Management account administrators or delegated administrators have permissions to archive and reactivate experiences..

> **Note**
>
> Before archiving an experience, you must disable it. For information about disabling an experience, see Configuring your private marketplace.
> If you're a current private marketplace customer without the AWS Organizations integration for private marketplace, administrators from the account that created the experience have permissions to archive and reactivate experiences.

To archive one or more private marketplace experiences

1. From the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane.
2. On the **Active experiences** tab, select one or more experiences.
3. Choose **Archive experience**.

   > **Note**
   >
   > If one or more of the experiences has a Live status, you must take them offline by choosing **Take experience(s) offline**.

4. To verify that you want to archive the experience, type **`confirm`** (all lowercase) in the text box.
5. Choose **Archive**.

   > **Note**
   >
   > You can also archive an experience by selecting the experience, choosing **Archive experience** under **Admin** mode on the **Settings** tab, and then choosing **Save**.

To reactivate one or more private marketplace experiences

1. From the Private Marketplace administrator's page, select **Experiences** in the left navigation pane.

2. On the **Archived experiences** tab, select one or more experiences.
3. Choose **Reactivate**.
4. To verify that you want to reactivate the experience, type **`confirm`** in the text box.
5. Choose **Reactivate**.

> **Note**
>
> You can also reactive an experience by selecting the experience, choosing **Reactivate experience** under **Admin** mode in the **Settings** tab, and then choosing **Save**.

Private offers

The AWS Marketplace seller private offer feature enables you to receive product pricing and EULA terms from a seller that aren't publicly available. You negotiate pricing and terms with the seller, and the seller creates a private offer for the AWS account that you designate. You accept the private offer and start receiving the negotiated price and terms of use.

Each private offer has pricing and licensing terms specifically offered to your account. The seller of the product extends a private offer to you, and the offer has a set expiration date. If you don't accept the private offer by the expiration date, depending on the type of product the private offer is for, you're either automatically moved to the product's public offer or no longer subscribed to the product.

If you're using the consolidated billing feature in AWS Organizations, you can accept the private offer from either the organization's management account or from a member account. If you accept from the management account, the private offer can be shared with all member accounts in the organization. Member accounts that were previously subscribed to the product must also accept the new private offer in order to benefit from pricing. Alternatively, for AMI and Container products, you can share the license from the management account to member accounts using AWS License Manager. Member accounts that weren't previously subscribed to the product must accept the private offer to be able to deploy the product.

For more information on consolidated billing, see Consolidated Billing for Organizations in the *AWS Billing User Guide*. The following are key points to remember as you start using your private offers.

- AWS Marketplace buyers can access third-party financing services for private offers. For more information, see Customer financing is now available in AWS Marketplace.
- There is no difference in the software product you purchase using a private offer. The software that you purchase using a private offer behaves the same as it would if you purchased the software without a private offer.
- Products subscriptions you purchase with a private offer show up like any other AWS Marketplace product in your monthly bill. You can use detailed billing to view your usage for each of your AWS Marketplace-purchased products. Each of your private offers has a line item corresponding to each kind of usage.
- Subscribing to a private offer doesn't require launching a new instance of the software. Accepting the private offer modifies the price to correspond to your private offer price. If a

product offers 1-click launch, you can deploy a new instance of the software. If a product defaults to 1-click launch, you can accept a private offer without launching a new instance. To launch without deploying a new instance, choose **Manual Launch** on the fulfillment page. You can use the Amazon Elastic Compute Cloud console to deploy additional instances, just as you would for other AWS Marketplace products.

- When a seller extends a private offer to you, you receive confirmation on the account the seller included in a private offer. Private offers are linked to the specific software buyer's account listed. The software seller creates the private offer for the account that you specify. Each private offer can be made to up to 25 accounts.
- When you accept a private offer, it becomes an *agreement* (also known as *contract* or *subscription*) between you and the seller.
- Sellers may offer to upgrade or renew your purchase of an SaaS contract or SaaS contract with consumption product. For example, a seller can create a new private offer to grant new entitlements, offer pricing discounts, adjust payment schedules, or change the end user license agreement (EULA) to use standardized license terms.

  These renewals or upgrades are changes to the original private offer that you accepted, and you use the same process for accepting them. If you accept the new upgrade or renewal private offer, the new agreement terms take effect immediately, without any break in software service. Any previous terms or remaining scheduled payments are cancelled and replaced by this new agreement's terms.
- You can review all of your annual software subscriptions in AWS Marketplace under **Your Software**. If an annual subscription is purchased by one account using AWS Organizations for consolidated billing, it is shared across the entire linked account family. If the purchasing account doesn't have any running instances, the annual subscription is counted toward the usage in another linked account running that software. For more information about annual subscriptions, see the section called “AMI subscriptions”.
- When a private offer expires, you can't subscribe to it. However, you can contact the seller. Ask the seller to change the expiration date on the current offer to a future date or create a new private offer for you.

Product types eligible for private offers

You can get private offers for the following product types.

Offer type	Description
Data products	For more information, see Accepting a Private Offer in the *AWS Data Exchange User Guide*.
SaaS contract	With a software as a service (SaaS) contract, you can commit to upfront payment for your expected usage of a SaaS product, or negotiate a flexible payment schedule with the seller. Contract durations are one-month , one-year, two-year, or three-year terms, or select a custom duration in months, up to 60 months. If you commit to an upfront payment, you are billed in advance for the use of the product software. If the seller offers a flexible payment schedule, you are billed along the payment schedule dates at the amounts listed on the private offer. The seller may also include negotiated pay-as-you-go pricing for usage above your contracte d usage.
SaaS subscription	With a SaaS subscription, you agree to a price for use of a product. The seller tracks and reports your usage to AWS Marketplace, and you're billed for what you use.
AMI hourly	With Amazon Machine Image (AMI) hourly, you negotiate an hourly rate for using an AMI, rounded up to the nearest hour.
AMI hourly with annual	With AMI hourly with annual, you negotiate the hourly and long-term pricing per instance type. The long-term pricing is for the duration of the private offer, which can be between 1

Offer type	Description
	day and 3 years. If the seller creates a private offer without a flexible payment schedule, you can run Amazon EC2 instances at the hourly price determined in the private offer and optionally purchase upfront commitmen ts for the duration of the contract at the long-term price set in the private offer. If the seller creates a private offer with a flexible payment schedule, you are billed with the payment schedule dates for the amounts listed on the private offer regardless of usage. In this type of private offer, the seller can include a number of Amazon EC2 instances per instance type that you can run without being charged the hourly price. Any usage above what is included is then charged at the hourly price set in the private offer.
AMI contract	With AMI contracts, you negotiate a contract price and the duration of the contract, which can be between 1 and 60 months. If the seller creates a private offer without a flexible payment schedule, at the time of acceptanc e, you can configure the contract according to the price and options set in the private offer. If the seller creates a private offer with a flexible payment schedule, you are billed with the payment schedule dates at the amounts listed on the private offer. In this type of private offer, the seller configures the contract in the private offer and it can't be configured at the time of acceptance.

Offer type	Description
Container products	With container products, you negotiate hourly or annual pricing for the container products that you use, by pod, task, or custom unit, matching the product that you are purchasin g. Container product private offers match AMI product private offers.
Machine learning products	Private offers can be a contract with a fixed upfront fee for a specified number of days. At the end of the contract, any instances that continue to run are billed at the hourly rate that the seller sets in the private offer.
Professional services	All professional services offers are private offers. You must work with the buyer to create the private offer. See Professional services products for more information.

Preparing to accept a private offer

When a typical private offer is negotiated, you pay the entire amount of the offer when you accept it, unless you are using third-party financing. With third-party financing, the financier pays the contract on your behalf and invoices you based on the agreed payment schedule. Before you accept a private offer, verify the billing structure for your company, your method of payment for AWS billing, and your tax settings.

> **Note**
>
> Certain sellers offer the option to request a private offer for their product on AWS Marketplace. For participating sellers, a **Request private offer** button will display on the product detail page. To request a private offer, choose the button and provide request details. You'll receive a confirmation email summarizing your request, and an AWS representative will contact you.

Verifying your AWS Billing and Cost Management preferences

Billing and Cost Management is the service that you use to pay your AWS bill, monitor your usage, and budget your costs. You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a management account that pays the charges of all the member accounts. The management account is called a payer account, and the member account is called a linked account. Before negotiating a private offer, verify how your company pays their AWS bill and which AWS account the private offer is made to.

Verifying your payment method

Before accepting a private offer, verify that your payment method supports paying the entire cost of the private offer. To verify your payment method, open the Billing and Cost Management console at https://console.aws.amazon.com/billing/.

Verifying your tax settings

If your company qualifies for a tax exemption, verify your tax settings. To view or modify your tax settings, sign in to the AWS Management Console and, in your account settings, view the tax settings. For more information on tax registration, see How do I add or update my tax registration number or business legal address for my AWS account?.

Viewing and subscribing to a private offer

You can view a private offer in one of the following ways:

Topics

- Viewing and subscribing to a private offer from a list of private offers
- Viewing and subscribing to a private offer from a seller-provided link
- Viewing and subscribing to a private offer from the product page

Viewing and subscribing to a private offer from a list of private offers

To view and subscribe to a private offer from a list of private offers extended to your AWS account

1. Sign in to the AWS Marketplace console.

2. Navigate to the **Private offers** page.
3. From the **Private offers** page, on the **Available offers** tab, select the **Offer ID** for the offer of interest.
4. View and subscribe to the private offer.

Viewing and subscribing to a private offer from a seller-provided link

To view and subscribe to a private offer from a link that the seller has sent to you

1. Sign in to the AWS Marketplace console.
2. Follow the link sent by the seller to directly access the private offer.

> **Note**
>
> Following this link before logging into the correct account will result in a **Page not found** (404) error.
> For more information, see I get a Page not found (404) error when I click the offer ID to view the private offer.

3. View and subscribe to the private offer.

Viewing and subscribing to a private offer from the product page

To view and subscribe to a private offer from the product page

1. Sign in to the AWS Marketplace console.
2. Navigate to the product page for the product.
3. View the banner at the top of the page showing the private offer, Offer ID, and expiration for the offer.

> **Note**
>
> Future-dated private offers are listed as **Early renewals**. For more information, see the section called “Working with future dated agreements”.

4. Select the **Offer ID**.

5. View and subscribe to the private offer.

> **Note**
>
> If you have more than one private offer for that product, each offer appears under **Offer name**. If you have a current contract for that product, an **In use** icon appears next to that offer.

Troubleshooting private offers

If you encounter HTTP status code 404 (Not Found) issues or similar difficulties when working with **Private offers** in AWS Marketplace, consult the topics in this section.

Issues

- I get a Page not found (404) error when I click the offer ID to view the private offer
- None of these suggestions work

I get a Page not found (404) error when I click the offer ID to view the private offer

- Check that you're signed in to the correct AWS account. The seller extends private offers to specific AWS account IDs.
- Check if the offer exists under **Private offers** in the AWS Marketplace console. If you don't find the offer under **Private offers**, it could be because the seller extended the offer to a different AWS account ID. Check with the seller to confirm the AWS account ID to which the offer was extended.
- Check that the private offer has not expired by viewing the **Accepted and expired offers** tab under **Private offers** in the AWS Marketplace console. If the offer has expired, work with the seller to modify the expiration date of the offer or extend a new offer to your account.
- Check that the account ID is allowlisted to view the private offer. Some ISVs use limited listings. Ask the ISV if they have allowlisted your account to view the product. Allowlisting is necessary for limited listings of AMI products. If you're in an AWS organization, and the seller extends the offer to the management account, linked accounts must be allowlisted to subscribe. Otherwise,

the buyer's linked accounts that aren't allowlisted will get a Page not found (404) error when trying to view the offer.

- Check with your AWS administrator to confirm that you have `aws-marketplace:ViewSubscriptions` IAM permissions if you need to view the offer. For more information about AWS Marketplace security, see Security on AWS Marketplace.
- Check if you're using a private marketplace.
  - Ensure that the product is on the allowlist of your private marketplace (if applicable), so that you can purchase the product. If you're not sure, contact your system administrator to check.

None of these suggestions work

If none of the previous suggestions resolved the HTTP status code 404 (Not Found) error, try the following actions in your browser:

- Clear the cache.
- Delete cookies.
- Sign out, and then sign back in.
- Use an incognito or private browsing mode.
- Try a different browser. We don't recommend using Internet Explorer.

If you have completed all of the troubleshooting suggestions and are still receiving a **Page not found** error, send an email message to <mpcustdesk@amazon.com> for assistance.

Private offers page in AWS Marketplace

In AWS Marketplace, the **Private offers** page lists all the private offers that have been extended to your AWS account for both private and public products. All offers available to you are displayed for each product. You can accept one offer for each product.

Understanding the Private offers page

You can view your **Private offers** page by signing in to the AWS Marketplace console and navigating to **Private offers**. Private offers extended to your AWS account are listed under **Private offers**, including the offer ID, product, seller of record (ISV or channel partner), publisher, active

agreements (if applicable), and the offer expiration date. You can select the **Offer ID** for the offer of interest to view the offer details and subscribe to a private offer.

The **Private offers** page includes the following information:

- The **Available offers** tab lists the private offers extended to your account that are available to accept. The **Offer ID** link on this tab is the same link that the seller might have provided to you to access the private offer details.
- The **Accepted and expired offers** tab lists the offers that you accepted and resulted in an agreement being created. It also lists offers that reached the offer expiration date set by the seller. This tab can be useful to retrieve a previous offer-id and agreement-id (if available) when renewing with a seller. If the offer resulted in an agreement and the agreement is active, you can choose the agreement to view the subscription detail page.

> **Note**
>
> Future-dated private offers are listed as **Early renewals**. For more information, see the section called "Working with future dated agreements".

For more information about modifying, upgrading, or renewing a private offer, see Modifying or unsubscribing from a private offer.

Required permissions to view the Private offers page

To view the **Private offers** page in the AWS Marketplace console, you must have the following permissions:

- If you use AWS managed policies: `AWSMarketplaceRead-only`, `AWSMarketplaceManageSubscriptions`, or `AWSMarketplaceFullAccess`
- If you aren't using AWS managed policies: IAM action `aws-marketplace:ListPrivateListingsand` `aws-marketplace:ViewSubscriptions`

If you're unable to view the **Private offers** page, contact your administrator to set up the correct AWS Identity and Access Management (IAM) permissions. For more information about the necessary IAM permissions for AWS Marketplace, see AWS managed policies for AWS Marketplace buyers.

Subscribing to a SaaS private offer

For a software as a service (SaaS) private offer, the configuration options that are available depend on the contract that you might negotiate with the seller.

As shown in the following diagram, the **Private offer** page includes the following sections:

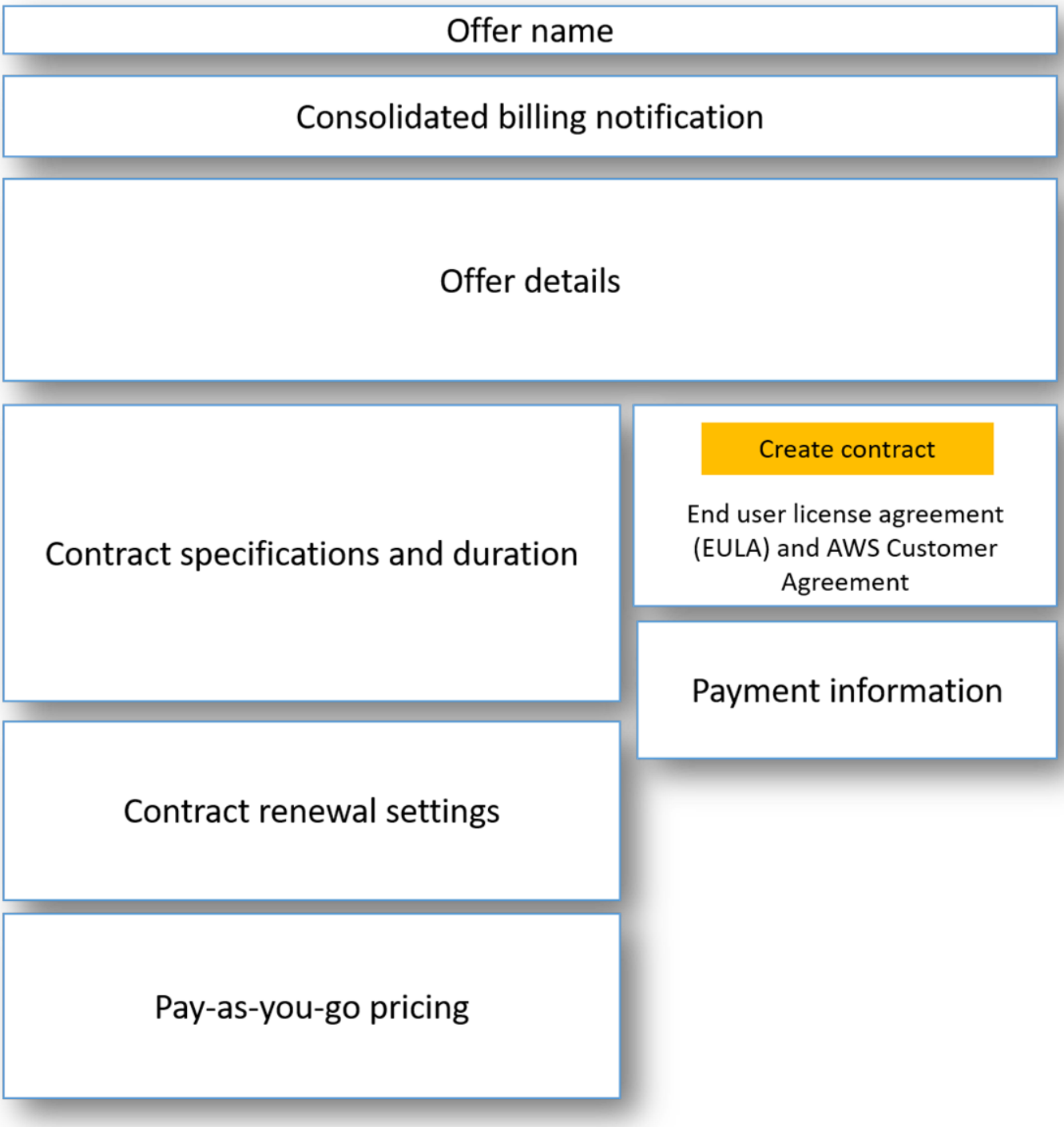
- **Offer name** – This is the name that the seller gave your private offer when they created it.
- **Consolidated billing information** – This notification appears if you're using consolidated billing with your AWS accounts.
- **Contract specifications and duration** – This pane shows the duration of the offer and the dimensions that define the offer. The dimensions describe how the usage is measured and the duration how long the negotiated pricing is in effect: for example, 5 GB/day for 12 months or $0.01 per user per hour. If the private offer is a contract, you pay for an agreed-to amount of usage over the duration of the contract. If the private offer is a subscription, you pay for your measured usage at the agreed-to rate.

  > **Note**
  >
  > Future-dated private offers are listed as **Early renewals**. For more information, see the section called “Working with future dated agreements”.

- **Contract renewal settings** – You can't set private offers to be renewed automatically. For private offers on SaaS products, this pane always indicates that there is no renewal for this offer.
- **Pay-as-you-go pricing** – If you negotiate pricing for product usage beyond what is defined in your private offer, the specifications for how much additional usage costs appear here. For example, if you agreed to a SaaS contract for data storage of 5 GB/day for 12 months and you use 10 GB/day, the first 5 GB fall under the contract. The additional 5 GB/day are charged at the pay-as-you-go price. With SaaS subscriptions, you have an agreed-to rate for however much you use during the duration of your contract.
- **End user license agreement (EULA) and contract creation button** – This is where you can view the license agreement that the seller uploaded for this private offer. This is also where you accept the contract after you have viewed all of the private offer specifications and are ready to enter into the contract.
- **Payment information** – This pane describes when payment is due and, if you negotiated a payment schedule, the date and times when payment is due.

Important

If a section doesn't appear on the **Private offer** page, then it isn't a negotiated part of the private offer.



To subscribe to a SaaS private offer

1. Follow the steps for Viewing and subscribing to a private offer.

2. In the offer details pane, verify that you chose the correct private offer. You might have multiple offers for the product.
3. In the contract specification and duration pane, verify that the contract duration and contract details are what you negotiated. If not, verify that you have selected the correct private offer or contact the seller who created the offer.

> **Note**
>
> Future-dated private offers are listed as **Early renewals**. For more information, see the section called "Working with future dated agreements".

4. If you negotiated pay-as-you-go pricing, there should be a pane with information that describes the terms that you negotiated. Verify the information, or if it's missing (and you expect it), contact the seller.
5. In the payment information pane, verify the payment information. If you negotiated a flexible payment schedule, the payment dates and amounts are listed. If you didn't, the total amount of the contract is billed when you accept the offer.
6. In the EULA and contract creation pane, validate that the EULA is the one you negotiated with the seller. After you review all of the terms and conditions for the contract, choose **Create contract** to accept the offer.

After you accept the offer, a confirmation page opens, indicating that you successfully subscribed to the product. Choose **Set Up Your Account** to be redirected to the seller's page and finish configuring your account on the seller's website.

Subscribing to an AMI private offer

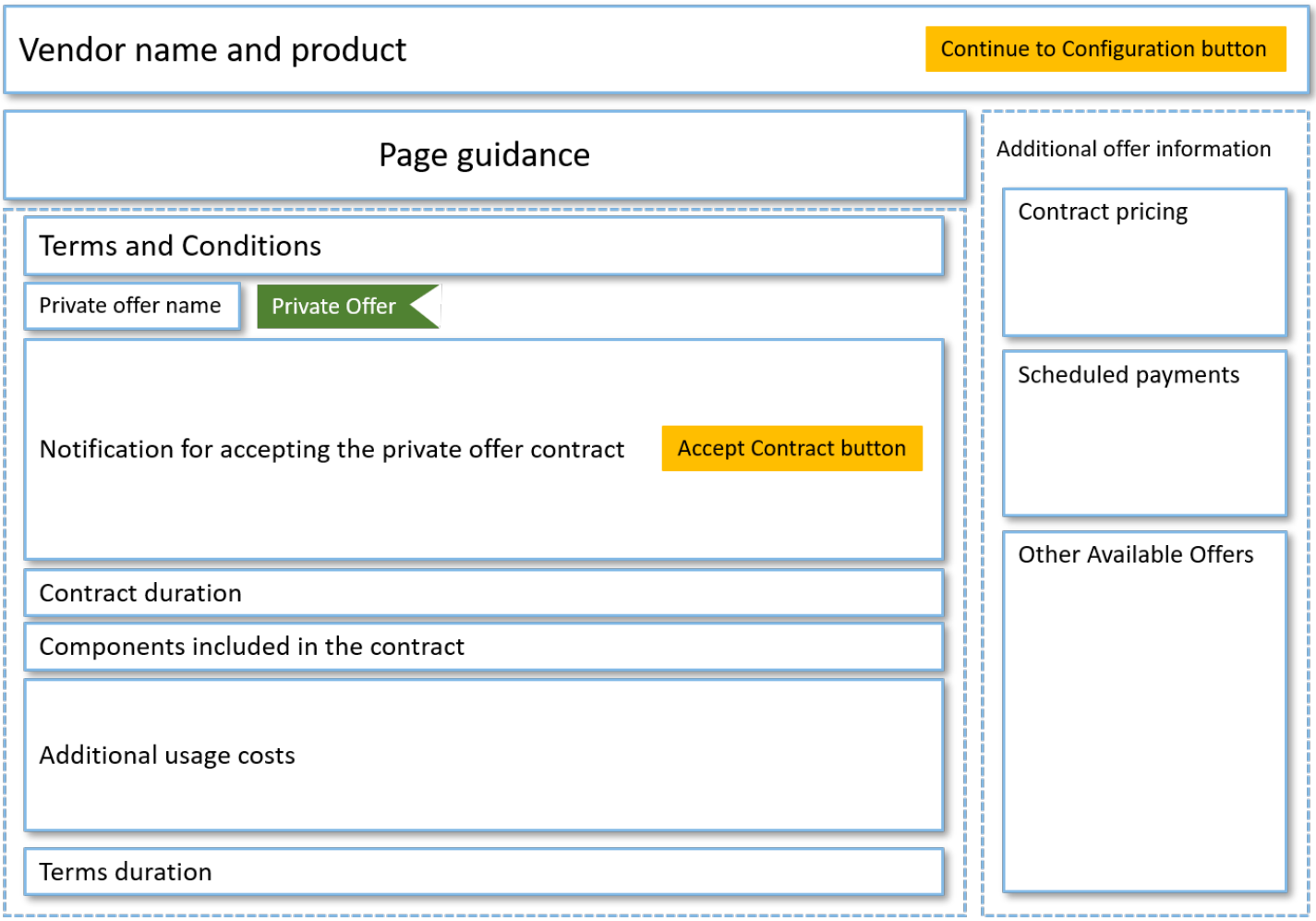
The sections and configuration options available for your Amazon Machine Image (AMI) private offer depend on the contract that you negotiate with the product vendor. The following image shows the layout for an AMI private offer page on the AWS Marketplace website.

As shown in the following diagram, the **Private offer** page includes the following sections:

- **Vendor name and product** – This is the name of the vendor and the product that the private offer is for. On the right is the configuration button for the product.
- **Page guidance** – This area has guidance for completing the tasks on the page and accepting the private offer.

- **Terms and conditions** – This section includes the following information:
  - In the upper left is the name of the private offer and a label indicating that this is a private offer.
  - Below the private offer name section is a notification for accepting the contract. You can use the **Accept Contract** button to accept the private offer.
  - Below the notification section are sections for the contract duration, components included in the contract, and the instance pricing you negotiated, along with another opportunity to view or download the EULA.
- **Terms duration** – This section shows the number of days of the contract and the end date of the contract.
- **Additional offer information** – On the right are thumbnail images of the total contract price, your next scheduled payment, the current terms, and other available private and public offers.

> **Note**
>
> If you're unable to access an instance type or AWS Region, it may not have been supported at the time the private offer was sent to you. Review your agreement details for more information. To obtain access to an instance or a Region, contact the seller and request an updated private offer. After you accept the new offer, you'll have access to the newly added instance or Region.



Subscribing to an annual AMI private offer with a flexible payment schedule

To subscribe to an AMI private offer, you must accept the private offer on the AWS Marketplace website. You can't accept the private offer on the AWS Marketplace console or the Amazon Elastic Compute Cloud (Amazon EC2) console. If the seller creates a private offer with a flexible payment schedule, you are billed with the payment schedule dates at the amounts listed on the private offer. To accept an AMI private offer with a flexible payment schedule, use the following procedure.

To accept an AMI private offer with a flexible payment schedule

1. Follow the steps for Viewing and subscribing to a private offer.
2. Verify that you're viewing the correct private offer. The vendor can create multiple private offers for you for their product. Any additional private offers appear in the **Other Available Offers** section.

3. Verify that the offer expiration date and the pricing information are what you negotiated for the private offer. If they aren't, verify that you're viewing the correct private offer.
4. Download the EULA, and verify that it's what you negotiated for the private offer.
5. In the **Terms duration** section, verify that the terms for the private offer are what you negotiated.
6. After you have verified the details for the private offer, in the **Terms and Conditions** section, choose **Accept Contract**.
7. Review the terms and choose **Confirm** if you accept.

> **Important**
>
> Do not refresh your browser while the system processes the request for your contract.

When you're ready to configure the AMI, choose **Continue to Configuration**. You must complete the subscription process for each use of the product.

Subscribing to an annual AMI private offer without a flexible payment schedule

To subscribe to an AMI private offer, you must accept the private offer on the AWS Marketplace website. You can't accept it on the AWS Marketplace console or the Amazon EC2 console. If the seller creates a private offer without a flexible payment schedule, at the time of acceptance, you can configure the contract according to the price and options set in the private offer. To accept an AMI private offer without a flexible payment schedule, use the following procedure.

To accept an AMI private offer without a flexible payment schedule

1. Verify that you're viewing the correct private offer. The vendor can create multiple private offers for you for their product. Any additional private offers appear in the additional private offers pane. Verify that the offer that you want to accept appears as **Viewing This Offer**.

> **Note**
>
> In many cases, the payer account isn't the account that uses the product. We recommend that you launch the product manually rather than selecting the one-click option if you accept the offer using the payer account.

2. Verify that the offer expiration date and the pricing information are what you negotiated for the private offer. If they aren't, verify that you're viewing the correct private offer.
3. Download the EULA, and verify that it's what you negotiated for the private offer.
4. In the contract terms pane, verify that the terms for the private offer are what you negotiated.
5. Verify that the offer details are what you negotiated for the private offer, and then choose **Accept Terms**. If they aren't, verify that you're viewing the correct private offer.
6. For **Subscribe to this software**, for **Instance type**, choose from the list of available instance types. For **Quantity**, choose the number of licenses.
7. Review your selections. When you are satisfied, choose **Create Contract**, and then choose **Confirm**.

When you're ready to configure the AMI, choose **Continue to Configuration**. You must complete the subscription process for each use of the product.

Modifying or unsubscribing from a private offer

You can update from standard subscriptions to private offers, and you can also modify certain existing private offers in AWS Marketplace. The process varies based on the agreement in place.

For many subscriptions, when you shift from public pricing to a private offer, you negotiate the offer with the ISV or your channel partner. After you accept the private offer, your related existing subscription or subscriptions automatically move to the private offer pricing model. This doesn't require any further action from you. Use the following guidance to identify your scenario and the steps to start receiving the pricing for your private offer.

Changing from public to private offer pricing

After you accept the private offer, no further action is needed for the user that accepted the offer. They are switched to the pricing, terms, and conditions defined in the private offer. To switch to the pricing, terms, and conditions for the private offer, each linked user using the product must accept the private offer. Any user that starts using the product must also accept the private offer to get the pricing, terms, and conditions defined in the private offer.

Changing a SaaS contract – upgrades and renewals

This section applies to software as a service (SaaS) contract and SaaS contract with consumption products. If you have an active contract in place from a previous private offer and you want to

accept a new private offer for the same product, the seller can upgrade or renew your existing agreement to modify the terms, pricing, or duration, or to renew your existing contract before it ends. This will result in a new private offer for you to accept, without needing to cancel your existing agreement first.

> **Note**
>
> Future-dated private offers are listed as **Early renewals**. For more information, see the section called "Working with future dated agreements".

To accept an upgrade or renewal, you must be on invoicing terms. If you're not currently on invoicing terms, submit a ticket to AWS Customer Service to change your payment method to invoicing.

If you don't want to switch to invoicing, then you can take either of the following actions:

- Work with the product vendor and AWS Marketplace customer support team to cancel the current contract before accepting a new private offer for that product
- Accept the offer on another AWS account.

Changing from a SaaS subscription to a SaaS contract

To change from a SaaS subscription to a SaaS contract, you must first unsubscribe from the SaaS subscription. Then you accept the private offer for the SaaS contract. To view your existing SaaS subscriptions, choose **Your Marketplace Software** in the upper-right corner of the AWS Marketplace console.

Changing from an AMI contract to a new contract

If you have an Amazon Machine Image (AMI) contract in place from a previous private offer and you want to accept a new private offer for the same product, you must do one of the following:

- Wait for the current AMI contract to expire before accepting the new AMI contract.
- Work with the product vendor and the AWS Marketplace customer support team to terminate your current contract.
- Accept the private offer using a different AWS account from the one that has the contract

Changing from AMI hourly to AMI annual

When you move from an AMI hourly subscription to an AMI annual subscription, the subscription works similar to a voucher system. Each hour of AMI usage is offset by one unit in the AMI annual subscription. When you purchase the annual subscription through a private offer, all associated accounts that are subscribed to the product are automatically switched to the pricing negotiated in the private offer. Linked accounts that start a subscription after the private offer is in place must subscribe to the private offer when they subscribe.

> **Note**
>
> The annual licenses on your old offer are deactivated immediately upon acceptance of the terms of the new offer. Work with the ISV to discuss compensation for the old licenses and how to proceed forward with the new offer.

Changing from AMI annual to AMI hourly

When your annual subscription expires, any linked accounts subscribed to the product are automatically switched to the AMI hourly pricing. If an annual subscription is in place, the linked account can't switch to an hourly subscription for that product without canceling the subscription.

Working with future dated agreements and private offers

With future dated agreements (FDA) in AWS Marketplace, you can subscribe to products where the product usage begins at a future date. You can manage when you buy a product *independently* from when you pay for, and when you use the product.

FDA helps buyers perform the following actions independently for transactions on AWS Marketplace:

- Procure the product/book the deal by accepting the offer.
- Begin product usage (license/entitlement activation).
- Pay for a purchase (invoice generation).

FDA is supported on private offers, creating for software as a service (SaaS) products, for contract and contracts with consumption pricing (CCP), and with or without flexible payments.

When you use future dated agreements, keep the following dates in mind:

Agreement sign date

The date when you accepted the offer and when the agreement was created. This date is when the agreement ID is created.

Agreement start date

The date when your product usage begins. This is the future date or future start date. This is the date that your license/entitlement is activated.

Agreement end date

The date when the agreement ends. The agreement and the license/entitlement expire on this date.

For more information about using FDAs, see the following topics:

Topics

- Creating future dated agreements
- Using a flexible payment scheduler with future dated agreements
- Amending your future dated agreements
- Receiving notifications for future dated agreements

Creating future dated agreements

For SaaS contracts and contracts with consumption pricing, with and without a flexible payment schedule, the seller sets the agreement start date as part of generating a private offer. As a buyer, you must work with sellers to make sure that the start date meets your requirements.

To create a future dated agreement, use the following procedure. You can view your future dated agreements in the AWS Marketplace console on the **Manage Subscriptions** page.

To create a future dated agreement

1. Follow the steps for Viewing and subscribing to a private offer.
2. In the offer details pane, verify that you chose the correct private offer and that the agreement start date is correct. Future dated offers are marked as **Early Renewals** on the **Offer** drop-down menu.

> **Note**
>
> For SaaS products, on the agreement start date, you must make sure to complete setting up your account with the ISV. You can't complete this step before the agreement start date. For more information, see the section called “Subscribing to a SaaS private offer”

Using a flexible payment scheduler with future dated agreements

You can use the flexible payment scheduler with future dated agreements. You can set up payments for purchases at a time of your choosing between your agreement sign date and agreement end date. This approach includes payments before and after the agreement start date.

The seller of record creating the private offer chooses payment dates and amounts. For more details, see Flexible payment scheduler.

Amending your future dated agreements

You can increase your purchased units of a particular dimension in your FDA after the agreement start date. This option is possible when the agreement doesn't have a flexible payment schedule. For more details, see Flexible payment scheduler.

You will be charged the pro-rated amount on the agreement start date when your amendment is complete. If your start date is in the past, you'll be charged immediately.

Receiving notifications for future dated agreements

You receive email notifications that are sent to your designated root account for the following actions taken on your future dated agreements:

- Offer acceptance/agreement creation (agreement sign date)
- Upon license or entitlement activation (agreement start date)
- Reminders for agreements expiring 30, 60, or 90 days in advance
- Agreement expiration (agreement end date)
- Upon an agreement amendment or replacement

Sharing subscriptions in an organization

When you subscribe to products in AWS Marketplace, an agreement is created that grants you a license to use those products. If your AWS account is a member of an organization, you can share that license for Amazon Machine Image (AMI), container, machine learning, and data products with the other accounts in that organization. You must set up license support in AWS Marketplace, and then share this from within AWS License Manager.

> **Note**
>
> For more information about AWS Organizations, see the AWS Organizations User Guide. For more information about sharing licenses with your organization in AWS License Manager, see Granted licenses in the *AWS License Manager User Guide*.

The following video provides a walkthrough of the license sharing experience.

Distribute your AWS Marketplace License Entitlements (3:56)

The following topics outline the process of viewing, sharing, and tracking licenses across accounts.

Topics

- Prerequisites for license sharing
- Viewing your licenses
- Sharing your licenses
- Tracking license usage

Prerequisites for license sharing

Before you can share licenses in AWS Marketplace you must set up license sharing for your organization. Complete the following tasks to set up license sharing for your organization:

- Give AWS Marketplace permission to manage licenses on your behalf so that it can create the associated license grants when you purchase or share your licenses. For more information, see Using roles to share entitlements for AWS Marketplace.
- Set up AWS License Manager for first use. For more information, see Getting started with AWS License Manager in the *AWS License Manager User Guide*.

Viewing your licenses

AWS Marketplace automatically creates licenses for AMI, container, machine learning, software as a service (SaaS), and data products that you purchase. You can share those licenses with other accounts in your organization.

> **Note**
>
> Although licenses are created for SaaS products, the sharing of SaaS licenses is not currently supported.

You manage and share licenses using AWS License Manager. However, you can use AWS Marketplace to view the licenses for products that you purchased from within AWS Marketplace.

To view licenses for your subscribed products in AWS Marketplace

1. In AWS Marketplace, sign in and choose **Manage Subscriptions**.
2. You can view all licenses or view the license for a specific subscription.
   - To view all licenses
     - From the **Actions** menu, select **View Licenses** to view all AWS Marketplace managed licenses in the License Manager console.
   - To view licenses for a single subscription
     a. Choose the card of the product that you want to view to go to its product details page.
     b. From the **Actions** menu, select **View License** to view the license for that product in the License Manager console.

> **Note**
>
> You can also view granted licenses that have been aggregated from all accounts in your organization. For more information, see Granted licenses in the *AWS License Manager User Guide*.

Sharing your licenses

Only AMI, container, machine learning, and data products have licenses that can be shared.

Subscriptions in AWS Marketplace have an **Access level** shown in the product details:

- Products with an **Agreement** level have a license that you can use and share with other accounts in your organization.
- Products with an **Entitlement** level are licenses that have been shared with your account—you can use these products, but you can't share them.

AWS Marketplace supports grants, which share the use of a license directly with AWS Organizations, an AWS account, or an organizational unit using AWS License Manager. The grant activation process now includes additional options to replace grants that are activated for the same product sourced from AWS Marketplace. For more information, see Granted licenses in the *AWS License Manager User Guide*.

> **Note**
>
> For products that are restricted to specific AWS Regions, an account you share your license with can only activate the license if the account is within an allowed Region.

Tracking license usage

You can track your usage-based license metrics for AMI products with AWS License Manager by selecting the **Usage dashboard** tab in each respective license.

For more information about using License Manager to track your license usage, see Granted licenses in the *AWS License Manager User Guide*.

Buyer notifications for AWS Marketplace events

AWS Marketplace provides timely notifications through email, Amazon EventBridge events, and Amazon Simple Notification Service (Amazon SNS) topics.

Topics

Email notifications for AWS Marketplace events

As a buyer in AWS Marketplace, you receive an email notification when either of the following occurs:

- You accept an offer.
- A seller publishes a new private offer that is related to the private offer that you accepted previously or publishes an update to the previously accepted offer.

> **Note**
>
> Notifications are sent to the email address associated with the buyer AWS account ID. Certain email providers (for example, Google or Yahoo) may filter out your AWS Marketplace notification emails. If you haven't received notifications from AWS Marketplace, or if you see them in your spam folder, adjust your email settings. For example, see Google Group instructions or Yahoo instructions.

Amazon EventBridge notifications for AWS Marketplace events

AWS Marketplace is integrated with Amazon EventBridge, formerly called Amazon CloudWatch Events. EventBridge is an event bus service that you can use to connect your applications with data from a variety of sources. For more information, see the *Amazon EventBridge User Guide*.

As a buyer, you receive an *event* from AWS Marketplace every time a seller creates an offer and makes it available for purchase. The *event* contains details like the ID, expiration date, product details, and the seller's name.

Topics

AWS Marketplace Discovery API Amazon EventBridge events

This topic provides detailed information about each event listed in the following table.

Action by seller	Event received by buyer	Related topic
Creates an offer and makes it available for purchase	`Listing Available`	the section called "Events for new listings"

Events for new listings

When a seller creates an offer and makes it available for purchase, the buyer receives an event with the following detail type: `Listing Available`.

> **Note**
>
> For information on creating EventBridge rules, see Amazon EventBridge rules in the *Amazon EventBridge User Guide*.

The following is an example event body for a `Listing Available` event.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "Listing Available",
    "source": "aws.discovery-marketplace",
    "account": "123456789012",
    "time": "2023-08-26T00:00:00Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "requestId": "3d4c9f9b-b809-4f5e-9fac-a9ae98b05cbb",
        "catalog": "AWSMarketplace",
        "offer": {
```

```
            "id": "offer-1234567890123",
            "expirationDate": "2025-08-26T00:00:00Z"
        },
        "product": {
            "id": "bbbbaaaa-abcd-1111-abcd-666666666666",
            "title": "Product Title"
        },
        "sellerOfRecord": {
            "name": "Seller Name"
        }
    }
}
```

Integrating AWS Marketplace with procurement systems

You can configure the integration of AWS Marketplace and your Coupa or SAP Ariba procurement software. After you complete the configuration, users in your organization can use your procurement software to search and request a subscription to AWS Marketplace products. After the subscription request is approved, the transaction is completed, and the user is notified that the software subscription is available. When the user signs in to AWS Marketplace, the software product is listed as a purchased subscription and is available for use. Integration with your procurement system can also integrate your AWS Marketplace invoices with your purchase order system.

How procurement integration works

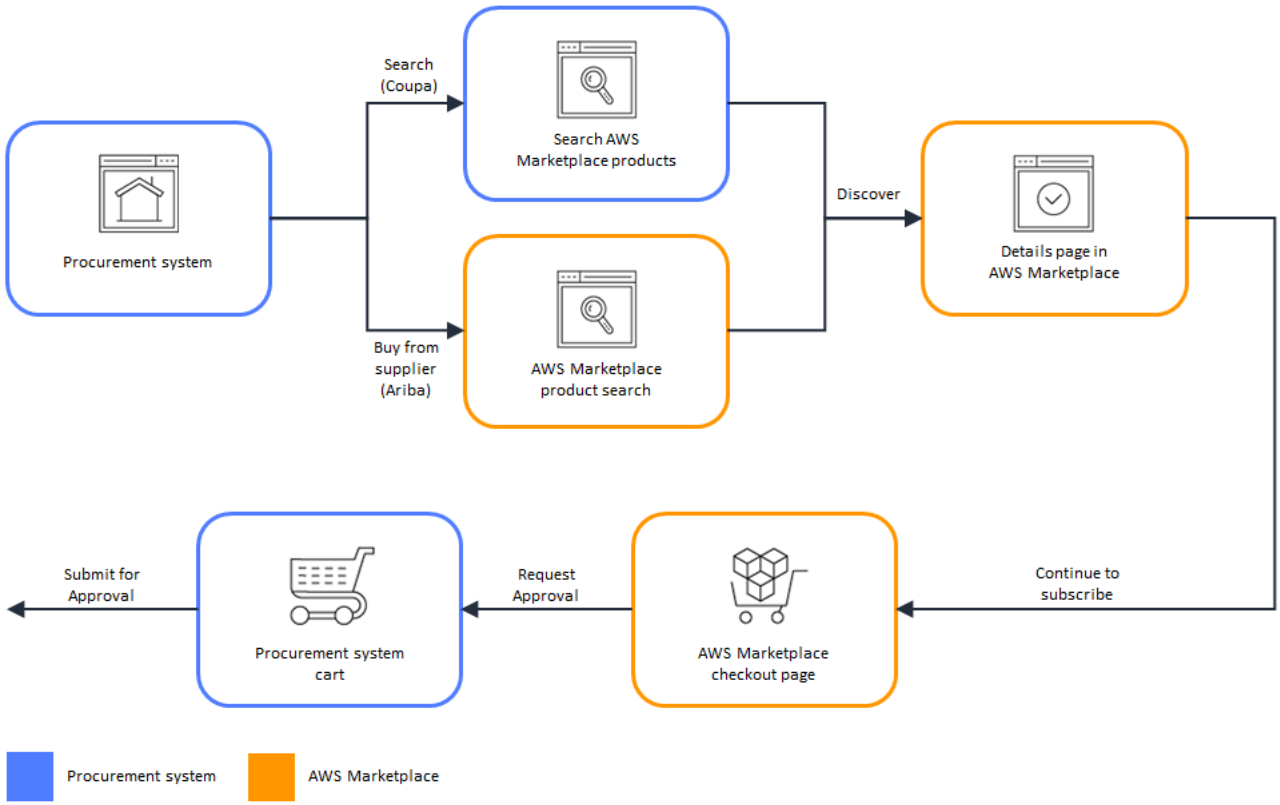
You can configure procurement software to integrate with AWS Marketplace following the commerce extensible markup language (cXML) protocol. This integration creates an access point into a third party's catalog, known as a *punchout*.

The integration differs slightly, based on the procurement system:

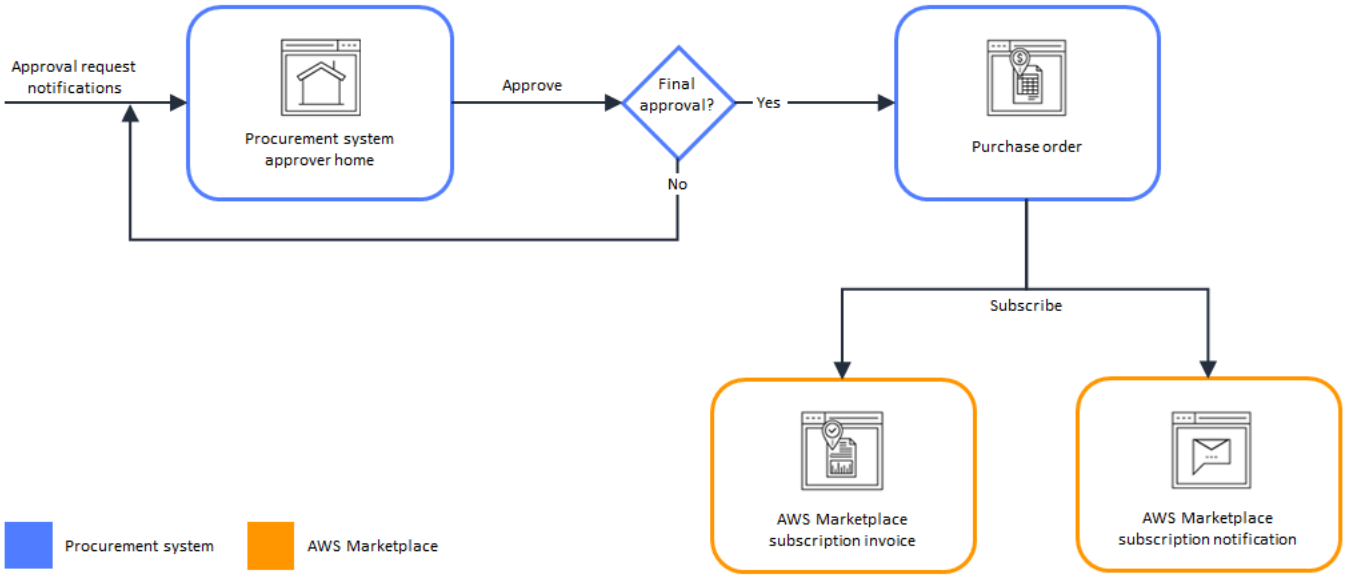
- **Coupa** – Using the Coupa Open Buy feature, you can search AWS Marketplace from within Coupa. Coupa displays search results, and when the user chooses a product, they're redirected to AWS Marketplace to see the details. Alternatively, users of Coupa's procurement software can access the AWS Marketplace catalog in the **Shop Online** section of their home page. The user can also choose to start directly in AWS Marketplace to browse for products.
- **SAP Ariba** – Ariba redirects users to AWS Marketplace to search for software and get details about a product. After an administrator configures the punchout integration, users of Ariba's procurement software can find AWS Marketplace software by choosing the **Catalog** tab, and then selecting the AWS Marketplace catalog. This redirects them to AWS Marketplace to find the products they're interested in.

  Ariba users must initiate their purchase from within Ariba, not AWS Marketplace.

When the user wants to purchase a subscription that they're browsing in AWS Marketplace, they create a subscription request within AWS Marketplace. On the product's subscription page, instead of completing the purchase, the user requests approval. The request is sent back to a shopping cart in the procurement system to complete the approval process. The following diagram shows the process for a procurement system subscription request.



When the procurement system receives the request from AWS Marketplace, the procurement system starts a workflow to complete the approval process. After the request is approved, the procurement system's purchase order system automatically completes the transaction on AWS Marketplace and notifies the user that their subscription is ready to deploy. The requester doesn't need to return to AWS Marketplace to complete the purchase. However, they may want to return to AWS Marketplace for instructions on how to use the product they have purchased. AWS Marketplace sends an email message to the AWS account used to access AWS Marketplace. The email message informs the recipient that the subscription succeeded and the software is available through AWS Marketplace. The following diagram shows the approval process for a procurement system subscription request.



Additional notes about integrating with procurement systems include the following:

- Free trials don't generate an invoice in the procurement system, because they don't have a charge associated with them.
- Contracts that have a one-time charge in addition to pay-as-you-go charges may require two sets of approvals. One approval is for the contract (or annual) price, and the other for the hourly or per-unit price (pay-as-you-go).
- Customers with PSI (Procurement System Integrations) can turn on pre-approvals for free products and BYOL products. There are two settings, one each for Free and BYOL. When the setting is enabled, orders are pre-approved in AWS Marketplace, and customers do not need to submit orders to their procurement system for approval. When the setting is disabled, customers will submit approvals via the **Request Approval** button to their procurement system. When the pre-approval setting for Free and BYOL products is disabled, $0.00 orders are produced in the customer's procurement system. For more information regarding Procurement System Integrations, see https://aws.amazon.com/marketplace/features/procurementsystem

Setting up procurement system integration

To configure the integration between AWS Marketplace and your procurement system, you start the process in AWS Marketplace and complete it in the procurement system. You use the information generated in AWS Marketplace to configure the procurement system punchout. To complete the configuration, the accounts that you use must meet the following requirements:

- The AWS account used to complete the AWS Marketplace configuration must be the management account and have the AWS Identity and Access Management (IAM) permissions defined in the `AWSMarketplaceProcurementSystemAdminFullAccess` managed policy.
- The procurement system account used to complete the configuration must have administration access to set up a contract, supplier, and punchout catalog in the procurement system.

Configuring IAM permissions

The following IAM permissions are in the AWS managed policy: AWSMarketplaceProcurementSystemAdminFullAccess managed policy and are required to configure the integration between AWS Marketplace and a procurement system.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

We recommend that you use IAM managed permissions rather than manually configuring permissions. Using this approach is less prone to human error, and if the permissions change, the managed policy is updated. For more information about configuring and using IAM in AWS Marketplace, see Security on AWS Marketplace.

Configuring AWS Marketplace to integrate with Coupa

After you have set up your IAM permissions, you are ready to configure AWS Marketplace integration with Coupa. Navigate to **Manage procurement**. In the **Manage procurement systems**

pane, enter a name and description for the punchout. You can also switch the integration to test mode so that users can test the integration without creating product subscriptions until you're ready. To configure the AWS Marketplace portion of the integration, complete the following procedure.

To configure AWS Marketplace for integrating with Coupa

1. From AWS Marketplace Manage Procurement Systems, under **Procurement systems**, choose **Set up Coupa integration**.
2. On the **Manage Coupa integration** page, under **Account information**, enter the name and description of your integration.

   > **Note**
   >
   > You might want your invoices in the AWS Billing console to reference the commerce extensible markup language (cXML) purchase order used to subscribe to your software as a service (SaaS) contract product. If so, you can enable the Billing integration using a service-linked role in AWS Marketplace settings.

3. You can turn on or turn off the configuration settings for **Enable redirect** and **Test mode**, and then select **Save** to complete the integration in the AWS Marketplace system.

After you have completed the integration in AWS Marketplace, you must go on to set up the integration in Coupa. You use the information generated on this page to configure the punchout in your Coupa system.

The AWS Marketplace configuration defaults to test mode being enabled. In test mode, subscription requests go to the Coupa backend so you can see the full flow, but a final invoice is not created. This helps you complete the configuration and enable the punchout in a planned manner.

> **Note**
>
> You can toggle testing mode on or off, as needed.
> Don't forget to turn off testing mode when you're finished with your integration.
> Otherwise, users in your system will appear to be creating requests, but no software will be purchased.

Configuring Coupa

To configure the integration with AWS Marketplace in your Coupa system, copy the information from the **Purchase information** pane of the **Manage Coupa integration** page in AWS Marketplace. Use this information to complete the steps in the following links that guide you through configuring your Coupa procurement system:

- Coupa Punchout Setup
- Configuring a Supplier for cXML Purchase Orders

> **Note**
>
> For information about UNSPSC codes used by AWS Marketplace, see UNSPSC codes used by AWS Marketplace .

Configuring AWS Marketplace to integrate with SAP Ariba

To configure AWS Marketplace to integrate with Ariba, you must work with the AWS Marketplace operations team to create a Level 1 punchout. For more information about SAP Ariba punchout, see Introduction to SAP Ariba PunchOut on the *SAP Community* website.

Gather the following information in preparation for configuring the setup:

- Your AWS account ID. If your AWS account is part of an AWS organization, then you also need the management account ID.
- The Ariba network ID (ANID) for your SAP Ariba system.

> **Note**
>
> For information about ANIDs in Ariba, and answers to other questions about Ariba see the Ariba Network for Suppliers: Frequently Asked Questions page on the *SAP Ariba* website.

To configure AWS Marketplace for integrating with Ariba

1. From AWS Marketplace Manage Procurement Systems, under **Procurement systems**, choose **Set up Ariba integration**.
2. On the **Manage SAP Ariba integration** page, under **Account information**, enter the name and description of your integration, as well as the **SAP Ariba Network ID** (ANID) for your Ariba system.

   > **Note**
   >
   > You might want your invoices in the AWS Billing console to reference the cXML purchase order used to subscribe to your SaaS contract product. If so, you can enable the Billing integration using a service-linked role in AWS Marketplace settings.

3. Make sure that **Test mode** is enabled, then select **Save** to save your AWS Marketplace integration settings.
4. Contact us to start the process of creating your SAP Ariba integration. Include the above information. AWS Marketplace sends you instructions for setting up and testing your Ariba integration.

> **Note**
>
> You need to have administrator access to your SAP Ariba system to create the *Supplier Relationship* with AWS Marketplace.

Following the instructions and configuration settings from the AWS Marketplace team, you create the integration in your SAP Ariba test environment, with AWS Marketplace running in *test mode*. In the test environment, subscription requests go to the Ariba backend so you can see the full flow including approvals, without creating a subscription in AWS Marketplace, and no invoice is generated. This approach enables testing the configuration prior to enabling the punchout in production. After your testing is complete and you are ready to move to production, contact us to set up the account in the production environment.

> **Note**
>
> Don't forget to move to production when you're finished with testing your integration. Otherwise, users in your system will believe that they're creating requests, but no software will be purchased.

When your testing is complete, and you have worked with the AWS Marketplace team to turn off test mode, your integration is complete.

For more information about configuring SAP Ariba, see the following topics from SAP Ariba:

- SAP Ariba PunchOut on the *SAP Ariba* website
- Introduction to SAP Ariba PunchOut on the *SAP Community* website

> **Note**
>
> For information about UNSPSC codes used by AWS Marketplace, see UNSPSC codes used by AWS Marketplace.

UNSPSC codes used by AWS Marketplace

AWS Marketplace uses the following United Nations Standard Products and Services code (UNSPSC) for software listings that are sent back to the procurement cart: 43232701

Disabling procurement system integration

To disable integration with either Coupa or SAP Ariba, you must remove the punchout integration from within the procurement system. To do this, disable the auto-redirect functionality for AWS Marketplace from within either Coupa or Ariba. This disables the integration, but maintains the settings and allows it to be re-enabled easily.

If you need to completely remove the integration setup on the AWS Marketplace side, you must contact us.

Free trials

Some products listed on AWS Marketplace offer free trials. The free trial enables you to try the software before you buy it. Free trials are limited to a certain amount of free usage, or for a specific amount of time. You can't pause a free trial period once it starts.

Software and infrastructure pricing

Free trials offered by sellers only apply to the software pricing of their product listed on AWS Marketplace. Buyers are responsible for all infrastructure costs while using a seller's product from AWS Marketplace regardless of whether the software pricing includes a free trial. These infrastructure costs are set by AWS and are available on their respective pricing pages. For example, if you subscribe to an Amazon Machine Image (AMI) product that has a free trial, you aren't charged for use of the AMI during the free trial. However, you might be charged for the Amazon Elastic Compute Cloud (Amazon EC2) instance on which you run the AMI product.

> **Note**
>
> Some products might require additional AWS infrastructure to perform. For example, sellers might provide deployment instructions or templates that deploy load balancers, storage, databases, or other AWS services into your AWS account. To understand what AWS services the seller has required for their product, review the detail pages for products listed on AWS Marketplace. Then, review the pricing pages of those AWS services.

Free trials for AMI-based products

Some AMI products with hourly or hourly with annual pricing in AWS Marketplace have free trials. When you subscribe to a free trial, you can run one Amazon EC2 instance of the AMI product for a duration set by the seller without incurring the hourly software charges. You're responsible for the infrastructure charge. Launching additional Amazon EC2 instances will incur the hourly software charge per instance. Free trials automatically convert to a paid subscription upon expiration.

If you don't terminate the Amazon EC2 instance before the free trial ends, you'll incur hourly software charges when the free trial ends. Unsubscribing to the free trial doesn't automatically end your Amazon EC2 instances, and you incur software charges for any continued use. For more information about infrastructure charges, see the Amazon EC2 pricing.

Free trials for container-based products

Some container products with hourly or hourly with long-term pricing in AWS Marketplace have free trials. When you subscribe to a free trial, you can run several Amazon Elastic Container Service (Amazon ECS) tasks or Amazon Elastic Kubernetes Service (Amazon EKS) pods for a duration without incurring hourly software charges. The number of tasks or pods included and the duration of the free trial are set by the seller. You're responsible for the infrastructure charge. Launching additional tasks or pods beyond the number included in the free trial will incur the hourly software charge per task or pod. Free trials automatically convert to a paid subscription upon expiration.

If you don't terminate the task or pod before the free trial ends, you'll incur hourly software charges when the free trial ends. Unsubscribing to the free trial doesn't automatically end your tasks or pods, and you incur software charges for any continued use. For more information about infrastructure charges, see Amazon ECS pricing and Amazon EKS pricing.

Free trials for machine learning products

Some machine learning products with hourly pricing in AWS Marketplace have free trials. When you subscribe to a free trial, you can run Amazon SageMaker endpoints, batch transform jobs, or training jobs for a duration set by the seller without incurring the hourly software charges. You're responsible for the infrastructure charge. Free trials automatically convert to a paid subscription upon expiration.

If you don't terminate any Amazon SageMaker endpoints, batch transform jobs, or training jobs before the free trial ends, you'll incur hourly software charges when the free trial ends. Unsubscribing to the free trial doesn't automatically end your Amazon SageMaker endpoints, batch transform jobs, or training jobs, and you incur software charges for any continued use. For more information about infrastructure charges, see Amazon SageMaker Pricing.

Free trials for SaaS products

Software as a service (SaaS) products in AWS Marketplace have free trials. SaaS free trials don't automatically convert into paid agreements. If you no longer want the free trial, you can let it expire. For more information, see SaaS free trials.

Using AWS free usage tier with AWS Marketplace

To help new Amazon Web Services (AWS) customers get started in the cloud, AWS introduced a free usage tier. The free tier can be used for anything you want to run in the cloud: launch new applications, test existing applications in the cloud, or simply gain hands-on experience with AWS. When the free usage period expires (or if the application use exceeds the free usage tier limits), you simply pay the standard, pay-as-you-go service rates. For more information, see AWS Free Tier.

AWS Free Tier customers are eligible to use free AWS Marketplace software for up to 750 hours of Amazon Elastic Compute Cloud (Amazon EC2) usage each month for one year. To get started, see AWS Marketplace.

Adding AWS Marketplace subscriptions to AWS Service Catalog

Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on Amazon Web Services (AWS). These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. Service Catalog allows you to centrally manage commonly deployed IT services. Service Catalog helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

For more information, see Adding AWS Marketplace products to your portfolio in the *Service Catalog Administrator Guide*.

Product reviews

AWS Marketplace wants buyers to get the information they need to make smart buying choices. As an AWS customer, you can submit written reviews for items listed in AWS Marketplace. We encourage you to share your opinions, both favorable and unfavorable.

> **Note**
>
> Data products don't support product reviews.

Guidelines

Anyone with an AWS Marketplace subscription to a product can create a review for it. Use the following guidelines for writing product reviews:

- *Include reasons* – The best reviews include not only whether you liked or disliked a product, but also why. You can discuss related products and how this item compares to them.
- *Be specific* – Focus on specific features of the product and your experience with it. For video reviews, write a brief introduction.
- *Be concise* – Written reviews must be at least 20 words and are limited to 5,000 words. The ideal length is 75–500 words.
- *Be sincere* – Your honest opinion about the product, positive or negative, is appreciated. Helpful information can inform our customers' buying decisions.
- *Be transparent* – If you received a free product in exchange for your review, clearly and conspicuously disclose that.

Restrictions

AWS reserves the right to remove reviews that include any of the following content.

- Objectional material, including:
  - Obscene or distasteful content
  - Profanity or spiteful remarks
  - Promotion of illegal or immoral conduct

- Promotional content, including:
  - Advertisements, promotional material, or repeated posts that make the same point
  - Sentiments by or on behalf of a person or company with a financial interest in the product or a directly competing product (including reviews by authors, publishers, manufacturers, or third-party merchants selling the product)
  - Reviews written for any form of compensation other than a free copy of the product, including reviews that are part of a paid publicity package
  - Reviews written by a customer without a verifiable subscription to the product
- Inappropriate content, including:
  - Content copied from others, including excessive quotations
  - Contact information or URLs external to Amazon.com
  - Details about availability or alternate ordering/shipping
  - Videos with watermarks
  - Comments on other reviews visible on the page, because page visibility is subject to change without notice
  - Foreign language content, unless there is a clear connection to the product
  - Text with formatting issues
- Off-topic information, including:
  - Feedback on the seller or your shipment experience
  - Feedback about typos or inaccuracies in our catalog or product description; instead, use the feedback form at the bottom of the product page

For questions about customer reviews, contact us.

Timing and expectations

We strive to process product reviews as quickly as possible. However, the AWS Marketplace team must communicate with both the reviewer and the seller to confirm and review the feedback for validity against our the section called “Guidelines” and the section called “Restrictions”. We follow the same timing and expectations guidance that is described in the *AWS Marketplace Seller Guide* for how long it will take to complete the process.

Getting support

For general AWS Marketplace issues, contact us. For questions about the software you purchase through AWS Marketplace, contact the software seller.

AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights simplifies software risk assessments by helping you to procure software that you trust and that meets your industry standards. With AWS Marketplace Vendor Insights, you can monitor the security profile of a product in near real-time from a single user interface. It reduces your assessment effort by providing a dashboard of a software product's security information. You can use the dashboard to view and evaluate information, such as data privacy, application security, and access control.

AWS Marketplace Vendor Insights gathers security data from sellers and supports buyers through procuring trusted software that continuously meets industry standards. By integrating with AWS Audit Manager, AWS Marketplace Vendor Insights can automatically pull up-to-date security information for your software as a service (SaaS) products in AWS Marketplace. AWS Marketplace Vendor Insights integrates with AWS Artifact third-party reports so you can access on-demand compliance reports for your vendor software, alongside reports for AWS services.

AWS Marketplace Vendor Insights provides evidence-based information from 10 control categories and multiple controls. It gathers the evidence-based information from three sources:

- **Vendor production accounts** – Of the multiple controls, 25 controls support live evidence gathering from a vendor's production accounts. Live evidence for each control is generated by one or more AWS Config rules that evaluate the configuration settings of a seller's AWS resources. Live evidence is the method of consistently updating data from multiple sources to present the most current information. AWS Audit Manager captures the evidence and delivers it to the AWS Marketplace Vendor Insights dashboard.
- **Vendor ISO 27001 and SOC 2 Type II reports** – The control categories are mapped to controls in the International Organization for Standardization (ISO) and Service Organization Control (SOC) 2 reports. When sellers share these reports with AWS Marketplace Vendor Insights, the service extracts the relevant data and presents it in the dashboard.
- **Vendor self-assessment** – Sellers complete a self-assessment. They can also create and upload other self-assessment types, including the AWS Marketplace Vendor Insights security self-assessment and Consensus Assessment Initiative Questionnaire (CAIQ).

The following video demonstrates how you can simplify the SaaS risk assessment and use AWS Marketplace Vendor Insights.

Getting started with AWS Marketplace Vendor Insights as a buyer

AWS Marketplace Vendor Insights presents security information for software products available in AWS Marketplace. You can use AWS Marketplace Vendor Insights to view security profiles for products in AWS Marketplace.

The AWS Marketplace Vendor Insights dashboard presents the compliance artifacts and security control information for a software product using AWS Marketplace Vendor Insights to assess the product. AWS Marketplace Vendor Insights gathers the evidence-based information for multiple security controls presented on the dashboard.

There is no charge for using AWS Marketplace Vendor Insights to access security and compliance information for products.

Find products with AWS Marketplace Vendor Insights

You can view profile and summary information for a product on the AWS Marketplace Vendor Insights dashboard or select the category controls and learn more about data gathered on the product. To find products in AWS Marketplace with AWS Marketplace Vendor Insights, use the following procedure.

To find products with AWS Marketplace Vendor Insights

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Choose **View all products**.
3. View products that have the **Vendor Insights** tag.
4. Under **Refine results for Vendor Insights**, choose **Security profiles**.
5. From the **Product detail** page, under **Product Overview**, choose **Vendor Insights** section.
6. Choose **View all profiles for this product**.
7. You can view details about the product in the **Overview** as well as a list of **Security certificates received**.
8. Choose **Request access**.
9. On the **Request access to Vendor Insights data** page, provide your information, and then choose **Request access**.

A success message appears, indicating that you have successfully requested access to the AWS Marketplace Vendor Insights data for this product.

Request access to assessment data by subscribing

With AWS Marketplace Vendor Insights, you can continuously monitor the security profile of vendor software. First, subscribe, or request access, to vendor assessment data for the product that you want to monitor. If you no longer want to monitor the assessment data for a product, you can unsubscribe from its assessment data. There is no charge for using AWS Marketplace Vendor Insights to access security and compliance information for products. For more information about pricing, see AWS Marketplace Vendor Insights Pricing.

To have access to all assessment data for a specific vendor product, you need to subscribe to the product's assessment data.

To subscribe to AWS Marketplace Vendor Insights assessment data for a product

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Choose **Vendor Insights**.
3. From **Vendor Insights**, choose a product.
4. Choose the **Overview** tab.
5. Choose **Request access**.
6. Enter your information in the fields provided.
7. When you're finished, choose **Request access**.

   A success message appears indicating you requested access to all vendor assessment data for this product.

Unsubscribe from assessment data

If you no longer want access to assessment data for a vendor product, you can unsubscribe from the product's assessment data.

To unsubscribe from AWS Marketplace Vendor Insights assessment data for a product

1. Sign in to the AWS Management Console and open the AWS Marketplace console.

2. Choose **Vendor Insights**.
3. From the **Product detail** page, choose a product, and then choose **Unsubscribe**.
4. Read the terms presented with unsubscribing to AWS Marketplace Vendor Insights data.
5. Type **`Unsubscribe`** in the text input field, then choose **Unsubscribe**.

   A success message appears, which indicates that you unsubscribed from AWS Marketplace Vendor Insights data and will no longer be charged for access.

Viewing a product's security profile with AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights gathers security data from sellers. A product's security profile displays updated information about the product's security, resiliency, compliance, and other factors needed for your assessment. This information supports buyers like you by helping you to procure trusted software that continuously meets industry standards. For each software as a service (SaaS) product that it assesses, AWS Marketplace Vendor Insights gathers the evidence-based information for multiple security controls.

Topics

- Dashboard in AWS Marketplace Vendor Insights
- View the security profile of a SaaS product
- Understanding control categories

Dashboard in AWS Marketplace Vendor Insights

The dashboard presents the compliance artifacts and security control information for a software product that is gathered by AWS Marketplace Vendor Insights. Evidence-based information for all security control categories is provided such as a change in data residency or certification expiration. The consolidated dashboard provides compliance information changes. AWS Marketplace Vendor Insights removes the need for you to create additional questionnaires and use risk assessment software. With a consistently updated and validated dashboard, you can continuously monitor the software's security control after procurement.

View the security profile of a SaaS product

AWS Marketplace Vendor Insights helps you make decisions about a seller's software. AWS Marketplace Vendor Insights extracts data from a seller's evidence-based information across 10 control categories and multiple controls. You can view profile and summary information for a SaaS product on the dashboard or select control categories to learn more about data gathered. You must be subscribed to the product and granted access to view compliance information through the profile.

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Choose **Vendor Insights**.
3. From **Vendor Insights**, choose a product.
4. On the **Profile detail** page, choose the **Security and compliance** tab.

> **Note**
>
> A number in a red circle indicates the number of non-compliant controls.

5. For **Control categories**, choose the text under any of the listed categories to view more information.
   - Choose the first control name (**Do you have a policy/procedure to ensure compliance with applicable legislative, regulatory and contractual requirements?**).
   - Read the information presented. You can also view reports from AWS Artifact third-party report or view exceptions from the auditor.
   - Select the product name in the navigation above to return to the **Product detail** page.

Understanding control categories

AWS Marketplace Vendor Insights provides you with evidence-based information from multiple controls within 10 control categories. AWS Marketplace Vendor Insights gathers the information from three sources: vendor production accounts, vendor self-assessment, and vendor ISO 27001 and SOC 2 Type II reports. For more information about these sources, see *AWS Marketplace Vendor Insights*.

The following list provides a description of each control category:

Access management

Identifies, tracks, manages, and controls access to a system or application.

Application security

Verifies if security was incorporated into the application when designing, developing, and testing it.

Audit, compliance, and security policy

Evaluates an organization's adherence to regulatory requirements.

Business resiliency and continuity

Evaluates the organization’s ability to quickly adapt to disruptions while maintaining business continuity.

Data security

Protects data and assets.

End user device security

Protects portable end user devices and the networks they are connected to from threats and vulnerabilities.

Human resources

Evaluates the employee related division for handling of sensitive data during processes such as hiring, paying, and terminating employees.

Infrastructure security

Protects critical assets from threats and vulnerabilities.

Risk management and incident response

Evaluates the level of risk deemed acceptable and the steps taken to respond to risks and attacks.

Security and configuration policy

Evaluates the security policies and security configurations that protect an organization's assets.

Control category sets

The following tables provide detailed information for each category with information about the values for each category gathered. The following list describes the type of information within each column of the table:

- **Control set** – Controls are assigned to a control set, and each control reflects the security function of its category. Each category has multiple control sets.
- **Control name** – Name of the policy or procedure. "Requires manual attestation" means written confirmation or documentation of the policy or procedure is required.
- **Control description** – Questions, information, or documentation needed about this policy or procedure.
- **Evidence extraction detail** – Information and context needed about the control to further obtain the data needed for this category.
- **Sample value** – Example given for guidance to what a compliance value for this category might look like so that it's in accordance with regulatory standards.

Topics

Access management controls

Access management controls identify, track, manage, and control access to a system or application. This table lists the values and descriptions for access management controls.

Control set	Control title	Control description
Secure authentication	Access Management 3.1.1 - Secure Authentication - Personal Data in UserId (Requires manual attestation)	Do you require personal data (oth email address) in the user ID?
	Access Management 3.1.2 - Secure Authentication - Application Supports Two Factor Authentication (Requires manual attestation)	Does the application support two- ation?
	Access Management 3.1.3 - Secure Authentication - Account Lockout (Requires manual attestation)	Is the customer's account locked i failed logins?
Credential management	Access Management 3.2.1 - Credential Management - Password Policy	Does the application have a strong
	Access Management 3.2.2 - Credential Management - Password Encryption	Does the password policy require ls (password and user ID) to be en and to be hashed with salt when s
	Access Management 3.2.3 - Credential Management - Secret Management	Do you use a secret management
	Access Management 3.2.4 - Credentia l Management - Credentials in Code (Requires manual attestation)	Are credentials included in the co
Access to production environment	Access Management 3.3.1 - Access to Production Environment - Single Sign-on (Requires manual attestation)	Is SSO enabled to access the prod nt?

Control set	Control title	Control description
	Access Management 3.3.2 - Access to Production Environment - Two Factor Authentication	Is two-factor authentication requi production or hosted environmen
	Access Management 3.3.3 - Access to Production Environment - Root User (Requires manual attestation)	Is root user used only by exceptio production environment?
	Access Management 3.3.4 - Access to Production Environment - Root User MFA	Does root user require multi-facto (MFA)?
	Access Management 3.3.5 - Access to Production Environment - Remote Access	Is remote access to the productio nt secured using mechanisms such channels or key based authenticat
Access control policy	Access Management 3.4.1 - Access Control Policy - Least Privilege Access	Do you follow least privilege acce to access the production environm
	Access Management 3.4.2 - Access Control Policy - Access Policy Review	Are all access policies in the produ reviewed regularly?
	Access Management 3.4.3 - Access Control Policy - Users and Security Policy Configuration (Requires manual attestation)	Does the application allow custom users and their privileges?
	Access Management 3.4.4 - Access Control Policy - Logical Segmentation (Requires manual attestation)	Is there logical segmentation of a

Control set	Control title	Control description
	Access Management 3.4.5 - Access Control Policy - Access Review upon Termination	Are all relevant access policies upo employee termination or change o
Access logs	Access Management 3.5.1 - Access Logs	Do you log activities performed by in the production environment?

Application security controls

Application security controls verify if security was incorporated into the application when designing, developing, and testing it. This table lists the values and descriptions for application security policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Secure software development lifecycle	Application Security 4.1.1 - Secure Software Developme nt Lifecycle - Separate Environment	Is the development, test, and staging environment separate from the production environment?	Specify if the development, test, and staging environment is separate from the production environment.	Yes
	Application Security 4.1.2 - Secure Software Developme nt Lifecycle - Secure Coding Practice	Do security engineers work with developer s on security practices?	Specify if developers and security engineer work together on secure coding practices.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.1.3 - Secure Software Development Lifecycle - Use of Customer Data in Test Environment (Requires manual attestation)	Is customer data ever used in the test, development, or QA environments?	Is customer data ever used in the test, development, or QA environments? If yes, what data is used and what is it used for?	No
	Application Security 4.1.4 - Secure Software Development Lifecycle - Secure Connection	Is SSL/TLS enabled for all web pages and communications that uses customer data?	Specify if a secure connection (such as SSL/TLS) is used for all communication with customer data.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.1.5 - Secure Software Development Lifecycle - Image Backup	Are application image snapshots backed up?	Specify if image snapshots (such as systems supporting the application and systems hosting customer data) are backed up. If yes, is there a process to ensure that image snapshots containing scoped data are authorized prior to being snapped? Is access control implemented for the image snapshots?	Yes. Images are backed up with customer's and management's approval.
Application security review	Application Security 4.2.1 - Application Security Review - Secure Code Review	Is secure code review done prior to each release?	Specify if a security code review is done prior to each release.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.2.2 - Application Security Review - Penetration Test	Are penetration tests performed ? Can we get reports of penetration testing?	Specify if penetrati on tests are performed on the applicati on. If yes, can you share the last 3 reports as manual evidence?	Yes
	Application Security 4.2.3 - Application Security Review - Security Patches	Are all available high-risk security patches applied and verified regularly ?	Specify if high-risk security patches are applied regularly . If yes, how often are they applied?	Yes. Security patches are applied monthly.
	Application Security 4.2.4 - Application Security Review - Vulnerabi lity Scans on Applications	Are vulnerability scans performed against all internet-facing applications regularly and after significant changes?	Specify if vulnerabi lity scans are performed on all internet-facing applications. If yes, how often are vulnerability scans done? Can we get a copy of the report?	Yes. Vulnerabi lity scans are performed monthly.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.2.5 - Application Security Review - Threats and Vulnerabilities Management	Are there processes to manage threat and vulnerability assessment tools and the data they collect?	Specify if there are processes to manage threat and vulnerabi lity assessment tools and their findings. Could you provide more details on how threats and vulnerabilities are managed?	Yes. All threats and vulnerabi lities from different sources are aggregated in one portal. They are managed by severity.
	Application Security 4.2.6 - Application Security Review - Anti Malware Scans	Is anti-malw are scanning done against the network and systems hosting the application regularly?	Specify if anti-malware scanning is done against the network and systems hosting the application. If yes, how often is it done? Can you provide the report?	Yes. Anti-malw are scans are performed monthly.
Application logs	Application Security 4.3.1 - Application Logs - Application Logs	Are application logs collected and reviewed?	Specify if application logs are collected and reviewed. If yes, how long are the logs retained?	Yes. Logs are retained for a year.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.3.2 - Application Logs - Access to Logs	Are operating system and application logs protected against modification, deletion, and/or inappropriate access?	Specify if operating system and application logs are protected against modification, deletion, and/or inappropriate access. In the event of a breach or incident, do you have processes in place to detect loss of application logs?	Yes
	Application Security 4.3.3 - Application Logs - Data Stored in Logs (Requires manual attestation)	Do you store customer's personally identifiable information (PII) in logs?	Specify if you store customer's personally identifiable information (PII) in logs.	No. No PII data will be stored in the logs.
Change control policy	Application Security 4.4.1 - Change Control Policy - Functional and Resiliency Testing	Is functional and resiliency testing done before releasing a change?	Specify if functional and resiliency testing is done on the application before a new release.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.4.2 - Change Control Policy - Change Control Procedures	Are change control procedures required for all changes to the production environment?	Specify if change control procedures are in place for all changes made in the production environment.	Yes
	Application Security 4.4.3 - Change Control Policy - Avoid Human Error/Risks in Production	Do you have a process in place to verify that human error and risks don't get pushed into production?	Specify that there's a process to verify that human error and risks don't get pushed into production.	Yes
	Application Security 4.4.4 - Change Control Policy - Document and Log Changes	Do you document and log changes that may impact services?	Specify if service-impacting changes are documented and logged. If yes, how long are the logs retained?	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Application Security 4.4.5 - Change Control Policy - Change Notification for Buyers (Requires manual attestation)	Is there a formal process to ensure customers are notified prior to changes being made which may impact their service?	Specify if customers will be notified prior to making changes that may impact their service. If yes, what is the SLA to notify customers about impacting changes?	Yes. We notify customers 90 days before impacting changes.

Audit and compliance controls

Audit and compliance controls evaluates an organization's adherence to regulatory requirements. This table lists the values and descriptions for audit and compliance controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Certifications completed	Audit and Compliance 1.1.1 - Certifications Completed (Requires manual attestation)	List certifications that you have.	Specify which certifications you have.	SOC2, ISO/IEC 27001
Certification in progress	Audit and Compliance 1.2.1 - Certifica	List additional certificates that	List any additional certificates that	Yes. PCI certification is in

Control set	Control title	Control description	Evidence extraction detail	Sample value
	tion in Progress (Requires manual attestation)	are currently in progress.	are currently being audited or reviewed with an estimated completion date.	progress (ETA Q2 2022).
Procedures ensuring compliance	Audit and Compliance 1.3.1 - Procedures ensuring Compliance - Procedures ensuring Compliance	Do you have a policy or procedure to ensure compliance with applicable legislative, regulatory, and contractual requirements?	Specify if you have a policy or procedure to ensure compliance with applicable legislative, regulatory, and contractual requirements. If yes, list details about the procedure and upload manual evidence.	Yes. We uploaded documents such as SOC2, ISO/IEC 27001.
	Audit and Compliance 1.3.2 - Procedures ensuring Compliance - Audits to Track Outstanding Requirements	Are audits completed to track outstanding regulatory and compliance requirements?	Specify if audits are done to track outstanding requirements. If yes, provide details.	Yes, audits are done monthly to track outstanding requirements.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Audit and Compliance 1.3.3 - Procedures ensuring Compliance - Deviations and Exceptions (Requires manual attestation)	Do you have a process to handle deviations and exceptions from compliance requirements?	Specify if there is a process to handle exceptions or deviations from compliance requirements. If yes, provide details.	Yes. We have a deviations log and reporting tools. We investigate every exception or deviation to prevent future occurrence.

Business resiliency controls

Business resiliency controls evaluate the organization's ability to quickly adapt to disruptions while maintaining business continuity. This table lists the values and descriptions for business resiliency policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Business resiliency	Business Resiliency and Continuity 6.1.1 - Business Resiliency - Failover Tests (Requires manual attestation)	Are site fail-over tests performed at least annually?	Specify if fail-over tests are performed annually. If no, how often are they performed?	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Business Resiliency and Continuity 6.1.2 - Business Resiliency - Business Impact Analysis (Requires manual attestation)	Has a business impact analysis been conducted?	Specify if a business impact analysis was done. If yes, when was it last completed ? Provide details on the analysis conducted.	Yes. A business impact analysis was completed 6 months ago.
	Business Resiliency and Continuity 6.1.3 - Business Resiliency - Dependencies on Third-Party Vendors (Requires manual attestation)	Are there any dependencies on critical third-party service providers (besides a cloud service provider) ?	Specify if there is any dependency on third-party vendors (besides a cloud service provider). If yes, can you provide details on the vendors?	No

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Business Resiliency and Continuity 6.1.4 - Business Resiliency - Third-Party Continuity and Recovery Tests (Requires manual attestation)	Do you require third-party vendors to have their own disaster recovery processes and exercises?	Specify if third-party vendors must have their own disaster recovery processes and exercises.	Not applicable in this sample.
	Business Resiliency and Continuity 6.1.5 - Business Resiliency - Third-Party Vendors Breach of Contract (Requires manual attestation)	Do contracts with critical service providers include a penalty or remediation clause for breach of availability and continuity Sold and Shipped by Amazon (SSA)?	Are penalty or remediation clauses for breach of availability and continuity included in contracts with third-party vendors?	Not applicable in this sample.
	Business Resiliency and Continuity 6.1.6 - Business Resiliency - Health of the System	Do you have monitors or alerts to understand the health of the system?	Specify if monitors or alerts are in place to understand the health of the system.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
Business continuity	Business Resiliency and Continuity 6.2.1 - Business Continuity - Business Continuit y Policies/ Procedures	Are formal business continuity procedures developed and documented?	Specify if formal procedures are developed and maintaine d for business continuity. If yes, provide more details on the procedures.	Yes
	Business Resiliency and Continuity 6.2.2 - Business Continuity - Response and Recovery Strategies	Are specific response and recovery strategies defined for the prioritized activities?	Specify if recovery and response strategies are developed for customer activities and services.	Yes
	Business Resiliency and Continuity 6.2.3 - Business Continuity - Business Continuity Tests	Do you perform recovery tests to ensure business continuity?	Specify if you perform recovery tests to ensure business continuity in case of a failure.	Yes. In case of a failure, systems for business continuity will be activated within 2 hours.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Business Resiliency and Continuity 6.2.4 - Business Continuity - Availabil ity Impact in Multi-Tenancy Environme nts (Requires manual attestati on)	Do you limit a buyer's ability to impose load that may impact availability for other users of your system?	Specify if one buyer's load can impact availabil ity for another buyer. If yes, what is the threshold until which there will be no impact? If no, can you provide more details on how you ensure services are not impacted during peak usage and above?	Yes. Threshold not available for this sample.
Application availability	Business Resiliency and Continuity 6.3.1 - Application Availability - Availability Record (Requires manual attestati on)	Were there any significant issues related to reliability or availability in the last year?	Specify if there were any significant issues related to reliability or availability in the last year.	No

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Business Resiliency and Continuity 6.3.2 - Application Availability - Scheduled Maintenance Window (Requires manual attestation)	Is downtime expected during scheduled maintenance?	Specify if there is a scheduled maintenance window during which services might be down. If yes, how long is the downtime?	No
	Business Resiliency and Continuity 6.3.3 - Application Availability - Online Incident Portal (Requires manual attestation)	Is there an online incident response status portal that outlines planned and unplanned outages?	Specify if there is an incident status portal that outlines planned and unplanned outages. If yes, provide details on how a customer can access it. How long after the outage will the portal be updated?	Yes. The customer can access details through example.com.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Business Resiliency and Continuity 6.3.4 - Application Availability - Recovery Time Objective (Requires manual attestation)	Is there a specific recovery time objective (RTO)?	Specify if there is a recovery time objective (RTO). If yes, can you provide the RTO?	Yes, a 2 hour RTO.
	Business Resiliency and Continuity 6.3.5 - Application Availability - Recovery Point Objective (Requires manual attestation)	Is there a specific recovery point objective (RPO)?	Specify if there is a recovery point objective (RPO). If yes, can you provide the RPO?	Yes, a 1 week RPO.

Data security controls

Data security controls protect data and assets. This table lists the values and descriptions for data security controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Customer data ingested	Data Security 2.1.1 - Customer	Create a list of data needed	Describe all data consumed	No sensitive and confidential data

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Ingested (Requires manual attestation)	from customers for product functionality.	from customers . Specify if sensitive or confidential data is consumed.	is consumed. This product only consumes non-sensitive information such as logs from applications, infrastructure, and AWS services. (AWS CloudTrail, AWS Config, VPC Flow Logs)
Data storage location	Data Security 2.2.1 - Data Storage Location (Requires manual attestation)	Where is customer data stored? List the countries and regions where data is stored.	Specify the list of countries and regions where data is stored.	Ohio (US), Oregon (US), Ireland (EU)
Access control	Data Security 2.3.1 - Access Control - Employee Access (Requires manual attestation)	Do employees have access to unencrypted customer data?	Specify if employees have access to unencrypted customer data. If yes, explain briefly why they need access. If no, explain briefly how you control access.	No, all data is encrypted when stored. Employees won't have access to customer data but only data about their usage.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Security 2.3.2 - Access Control - Mobile Application (Requires manual attestation)	Can customers access their data through a mobile application?	Specify if customers can access their data using a mobile application. If yes, provide more details. How do customers sign in? Are credentials cached by the application? How often are tokens refreshed?	No, service can't be accessed using a mobile application.
	Data Security 2.3.3 - Access Control - Countries Data is Transmitted to (Requires manual attestation)	Is customer data transmitted to countries outside the origin?	Is customer data transmitted to countries outside the origin? If yes, specify the list of countries where customer data is transmitted or received.	No

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Security 2.3.4 - Access Control - Is Data Shared with Third Party Vendors (Requires manual attestation)	Is customer data shared with third-party vendors (other than cloud service providers)?	Is customer data shared with third- party vendors? If yes, specify the list of third-party vendors and their countries or Region where you provide customer data.	No
	Data Security 2.3.5 - Access Control - Security Policy related to Third Party Vendors	Do you have policies or procedures in place to ensure that third-party vendors maintain the confidentiality, availability, and integrity of customer data?	Specify if you have policies or procedures in place to ensure that third-party vendors maintain the confidentiality, availability, and integrity of customer data. If yes, upload a manual or document of the policies or procedures.	Not applicable in this sample.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Data encryption	Data Security 2.4.1 - Data Encryption - Data Encryption at Rest	Is all data encrypted at rest?	Specify if all data is encrypted at rest.	Yes
	Data Security 2.4.2 - Data Encryption - Data Encryption in Transit	Is all data encrypted in-transit?	Specify if all data is encrypted in-transit.	Yes
	Data Security 2.4.3 - Data Encryptio n - Strong Algorithm s (Requires manual attestati on)	Do you use strong encryptio n algorithms?	Do you use strong encryptio n algorithms? If yes, specify what encryption algorithms (such as, RSA, AES 256) are used.	Yes. AES 256 is used for encrypting the data.
	Data Security 2.4.4 - Data Encryptio n - Unique Encryption Key (Requires manual attestati on)	Are customers provided with the ability to generate a unique encryptio n key?	Can customers provide or generate their own unique encryption keys? If yes, please provide more details and upload evidence.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Security 2.4.5 - Data Encryption - Encryption Keys Access (Requires manual attestation)	Are employees prevented from accessing a customer's encryption keys?	Specify if your employees are prevented from accessing a customer's encryption keys. If no, explain why they have access to customer keys. If yes, explain how access is controlled.	Yes. Cryptographic keys are securely stored and periodically rotated. Employees don't have access to these keys.
Data storage & classification	Data Security 2.5.1 - Data Storage & Classification - Data Backup	Do you back up customer data?	Specify if you back up customer data. If yes, describe your back up policy (including details about how often backup occurs, where the backup is stored, backup encryption and redundancy.)	Yes, backup is done every three months. Backup is encrypted and stored in the same region as the customer data. The customer's support engineer has access to restore the backup but not the data in the backup.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Security 2.5.2 - Data Storage & Classification - Data Access Control Policy	Do you implement appropriate access controls for stored customer data? Provide your access control policies.	Specify if appropriate access controls (such as RBAC) are implement ed for stored customer data. Provide more details and manual evidence on how you control access to the data.	Yes. The least privilege access controls are implemented to restrict access to customer data.
	Data Security 2.5.3 - Data Storage & Classification - Transaction Data (Requires manual attestati on)	Are the customer's transaction details (such as payment card information and informati on about the groups conducting transactions) stored in a perimeter zone?	Specify if the customer's transaction details (such as payment card information and informati on about the groups conducting transactions) will be stored in a perimeter zone. If yes, explain why it needs to be stored in the perimeter zone.	No

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Data Security 2.5.4 - Data Storage & Classification - Information Classification	Is customer data classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?	Specify if customer data is classified by sensitivity. If yes, upload manual evidence of this classification.	Yes
	Data Security 2.5.5 - Data Storage & Classification - Data Segmentation (Requires manual attestation)	Is data segmentation and separation capability between customers provided?	Specify if the data for different customers is segmented. If no, explain mechanisms you have to protect data from cross contamination.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
Data retention	Data Security 2.6.1 - Data Retention (Requires manual attestation)	How long do you retain data?	Specify the duration of data retention. If the retention period differs by data classification and sensitivity, can you provide details on each retention period?	6 months
Data retention after buyers unsubscribe	Data Security 2.6.2 - Data Retention after Client's Unsubscribe (Requires manual attestation)	How long do you retain data after buyers unsubscribe?	Specify the duration of data retention after customers unsubscribe.	3 months

End user device security controls

End user device security controls protect portable end user devices and the networks they are connected to from threats and vulnerabilities. This table lists the values and descriptions for end user device security policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Asset/software inventory	End User Device Security 7.1.1 -	Is the asset inventory	Specify if an asset inventory	Yes. Inventory is updated weekly.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Asset/Software Inventory - Asset Inventory	list updated periodically?	is maintained. If yes, how often is it updated?	
	End User Device Security 7.1.2 - Asset/Software Inventory - Software and Applications Inventory	Are all installed software platforms and applications on scoped systems inventoried?	Specify if inventory of all installed software and applications is maintained. If yes, how often is it updated?	Yes. Inventory is updated weekly.
Asset security	End User Device Security 7.2.1 - Asset Security - Security Patches	Are all available high-risk security patches applied and verified at least monthly on all end user devices?	Specify if all high risk security patches are applied at least monthly. If no, how often is it applied? Can you provide more details on how you manage patching?	Yes. We have a security team that performs this process bi-weekly.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	End User Device Security 7.2.2 - Asset Security - Endpoint Security	Do you have endpoint security?	Specify if endpoint security is installed on all devices. If yes, can you provide more details on the tool and how it is maintained?	Yes. Our security team handles this bi-weekly using internal tools.
	End User Device Security 7.2.3 - Asset Security - Maintenance and Repair of Assets (Requires manual attestation)	Is maintenance and repair of organizational assets performed and logged, with approved and controlled tools?	Specify if maintenance and repair of assets is performed and logged with controlled tools. If yes, could you provide more details on how it is managed?	Yes. All maintenance of devices is logged. This maintenance does not lead to downtime.
	End User Device Security 7.2.4 - Asset Security - Access Control for Devices	Do the devices have access control enabled?	Specify if devices have access controls (such as RBAC) enabled.	Yes. Least privilege access is implemented for all devices.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Device logs	End User Device Security 7.3.1 - Device Logs - Sufficient Details in Logs (Requires manual attestation)	Are sufficient details logged in operating system and device logs to support incident investigation?	Specify if sufficient details (like successful and failed login attempts and changes to sensitive configuration settings and files) are included in the logs to support incident investigation. If no, provide more details on how you handle incident investigations.	Yes
	End User Device Security 7.3.2 - Device Logs - Access to Device Logs	Are device logs protected against modification, deletion, and/or inappropriate access?	Specify if device logs are protected against modification, deletion, and/or inappropriate access. If yes, can you provide details on how you enforce it?	Yes. Changes to logs are enforced by access control. All changes to logs lead to an alert.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	End User Device Security 7.3.3 - Device Logs - Log Retention (Requires manual attestation)	Are logs retained for sufficient time to investigate an attack?	How long will the logs be retained?	Yes, 1 year.
Mobile device management	End User Device Security 7.4.1 - Mobile Device Management - Mobile Device Management Program	Is there a mobile device management program?	Specify if there is a mobile device management program. If yes, please specify what tool is used for mobile device management.	Yes. We use internal tools.
	End User Device Security 7.4.2 - Mobile Device Management - Access Production Environment from Private Mobile Devices (Requires manual attestation)	Are staff prevented from accessing the production environment by using unmanaged private mobile devices?	Specify if employees are prevented from accessing the production environment by using unmanaged private mobile devices. If no, how do you enforce this control?	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	End User Device Security 7.4.3 - Mobile Device Management - Access Customer Data from Mobile Devices (Requires manual attestation)	Are employees prevented from using unmanaged private mobile devices to view or process customer data?	Specify if employees are prevented from accessing customer data by using unmanaged mobile devices. If no, what is the use case for allowing access? How do you monitor access?	Yes

Human resources controls

Human resources controls evaluate the employee related division for handling of sensitive data during processes such as hiring, paying, and terminating employees. This table lists the values and descriptions for human resources policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Human resources policy	Human Resources 9.1.1 - Human Resources Policy - Background Screening for Employees	Is background screening done before employment?	Specify if background screening is done for all employees before employment.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Human Resources 9.1.2 - Human Resources Policy - Employee Agreement	Is an employmen t agreement signed before employment?	Specify if an employment agreement is signed before employment.	Yes
	Human Resources 9.1.3 - Human Resources Policy - Security Training for Employees	Do all employees undergo security awareness training regularly?	Specify if employees undergo security training regularly. If yes, how often do they undergo security training?	Yes. They undergo security training annually.
	Human Resources 9.1.4 - Human Resources Policy - Disciplinary Process for Non Compliance of Policies	Is there a disciplinary process for non-compliance of human resource policies?	Specify if there is a disciplinary process for non-compliance of human resource policies.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Human Resources 9.1.5 - Human Resources Policy - Background Checks for Contractors/ Subcontractors (Requires manual attestation)	Are background checks performed for third-party vendors, contractors, and subcontractors?	Specify if background checks are done for third-party vendors, contractors, and subcontractors. If yes, is the background check done regularly?	Yes. Background check is done annually.
	Human Resources 9.1.6 - Human Resources Policy - Return of Assets upon Termination	Is there a process to verify return of constituent assets upon termination?	Specify if there is a process to verify return of constituent assets upon employee termination.	Yes

Infrastructure security controls

Infrastructure security controls protect critical assets from threats and vulnerabilities. This table lists the values and descriptions for infrastructure security policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Physical security	Infrastructure Security 8.1.1 - Physical Security	Are individuals that require access to assets in-person (such	Specify if individuals that require access to assets in-	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	- Physical Access to Facilities	as buildings , vehicles, or hardware) required to provide ID and any necessary credentials?	person (such as buildings , vehicles, hardware) are required to provide ID and any necessary credentials.	
	Infrastructure Security 8.1.2 - Physical Security - Physical Security and Environmental Controls in Place	Are physical security and environmental controls in place in the data center and office buildings?	Specify if physical security and environme nt controls are in place for all the facilities.	Yes
	Infrastructure Security 8.1.3 - Physical Security - Visitor Access (Requires manual attestati on)	Do you record visitor access?	If visitors are permitted in the facility, are visitor access logs maintaine d? If yes, how long are the logs retained?	Yes. Logs will be maintained for a year.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Network security	Infrastructure Security 8.2.1 - Network Security - Disable Unused Ports and Services (Requires manual attestation)	Are all unused ports and services disabled from the production environment and systems?	Specify if all unused ports and services are disabled from the production environment and systems.	Yes
	Infrastructure Security 8.2.2 - Network Security - Use of Firewalls	Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?	Specify if firewalls are used to isolate critical and sensitive segments from segments with less sensitive systems.	Yes
	Infrastructure Security 8.2.3 - Network Security - Firewall Rules Review	Are all firewalls rules reviewed and updated regularly?	How often are firewall rules reviewed and updated?	Yes. Firewall rules are updated every 3 months.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Infrastructure Security 8.2.4 - Network Security - Intrusion Detection/ Prevention Systems	Are intrusion detection and preventio n systems deployed in all sensitive network zones and wherever firewalls are enabled?	Specify if intrusion detection and prevention systems are enabled in all sensitive network zones.	Yes
	Infrastructure Security 8.2.5 - Network Security - Security and Hardening Standards	Do you have security and hardening standards in place for network devices?	Specify if you have security and hardening standards in place for network devices. If yes, can you provide more details (includin g details about how often these standards are implemented and updated)?	Yes. Security and hardening standards are implemented on network devices monthly.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Cloud services	Infrastructure Security 8.3.1 - Cloud Services - Platforms Used to Host Applicati on (Requires manual attestati on)	List the cloud platforms you use for hosting your application.	Specify which cloud platforms you use for hosting your application.	AWS

Risk management and incident response controls

Risk management and incident response controls evaluate the level of risk deemed acceptable and the steps taken to respond to risks and attacks. This table lists the values and descriptions for risk management and incident response policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Risk assessment	Risk Managemen t/Incident Response 5.1.1 - Risk Assessmen t - Address and Identify Risks	Is there a formal process focused on identifying and addressing risks of disruptiv e incidents to the organizat ion?	Specify if there is a process to identify and address risks that cause disruptive incidents for the organization.	Yes
	Risk Managemen t/Inciden t Response 5.1.2 - Risk Assessment -	Is there a program or process to manage the treatment of	Specify if there is a program or process to manage risks and their	Yes. We regularly review and remediate issues to address non-confo

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management Process	risks identified during assessments?	mitigations. If yes, can you provide more details about the risk management process?	rmities. The following information is identified for any issue that affects our environment: • Details of issue identified • Root cause • Compensating controls • Severity • Owner • Near term path forward • Long term path forward
	Risk Management/Incident Response 5.1.3 - Risk Assessment - Risk Assessments	Are risk assessments done frequently?	Are risk assessments done frequently? If yes, specify the frequency of risk assessments.	Yes. Risk assessments are completed every 6 months.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management/Incident Response 5.1.4 - Risk Assessment - Third-Party Vendors Risk Assessment	Are risk assessments performed for all third-party vendors?	Specify if risk assessments are performed for all third-party vendors. If yes, how often?	Not applicable in this sample.
	Risk Management/Incident Response 5.1.5 - Risk Assessment - Risk Reassessment when Contract Changes	Are risk assessments performed when service delivery or contract changes occur?	Specify if risk assessments will be performed every time a service delivery or contract changes.	Not applicable in this sample.
	Risk Management/Incident Response 5.1.6 - Risk Assessment - Accept Risks (Requires manual attestation)	Is there a process for management to knowingly and objectively accept risks and approve action plans?	Specify if there is a process for management to understand and accept risks, and to approve action plans and a time line to fix a risk-related issue. Does the process include providing details of the metrics behind each risk to the management?	Yes. Details about risk severity and the potential issues if it's not mitigated are provided to management before they approve a risk.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management/Incident Response 5.1.7 - Risk Assessment - Risk Metrics (Requires manual attestation)	Do you have measures in place to define, monitor, and report risk metrics?	Specify if there is a process to define, monitor, and report risk metrics.	Yes
Incident management	Risk Management/Incident Response 5.2.1 - Incident Management - Incident Response Plan	Is there a formal Incident Response Plan?	Specify if there is a formal Incident Response Plan.	Yes
	Risk Management/Incident Response 5.2.2 - Incident Management - Contact to Report Security Incidents (Requires manual attestation)	Is there a process for customers to report a security incident?	Specify if there is a process for customers to report a security incident. If yes, how can a customer report security incident?	Yes. Customers can report incidents to example.com.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management/Incident Response 5.2.3 - Incident Management - Report Incidents /Key Activities	Do you report key activities?	Do you report key activities? What is the SLA for reporting key activities?	Yes. All key activities will be reported within a week.
	Risk Management/Incident Response 5.2.4 - Incident Management - Incident Recovery	Do you have disaster recovery plans?	Specify if you have plans for recovery after an incident occurs. If yes, can you share details about the recovery plans?	Yes. After an incident, recovery will be done within 24 hours.
	Risk Management/Incident Response 5.2.5 - Incident Management - Logs Available to Buyers in case of an Attack (Requires manual attestation)	In case of an attack, will relevant resources (such as logs, incident report, or data) be available to customers?	Will relevant resources (such as logs, incident report, or data) related to their use be available to customers in case an attack or incident occurs?	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management/Incident Response 5.2.6 - Incident Management - Security Bulletin (Requires manual attestation)	Do you have a security bulletin that outlines latest attacks and vulnerabilities affecting your applications?	Specify if you have a security bulletin that outlines latest attacks and vulnerabilities affecting your applications. If yes, can you provide the details?	Yes. Customers can report incidents to example.com.
Incident detection	Risk Management/Incident Response 5.3.1 - Incident Detection - Comprehensive Logging	Is there comprehensive logging to support the identification and mitigation of incidents?	Specify if there is comprehensive logging enabled. Identify the types of events that the system is capable of logging. How long are logs retained?	Yes. The following events are logged: applications, device, and AWS services such as AWS CloudTrail, AWS Config, and VPC Flow Logs. Logs are retained for 1 year.

Control set	Control title	Control description	Evidence extraction detail	Sample value
	Risk Management/Incident Response 5.3.2 - Incident Detection - Log Monitoring	Do you monitor and alert on unusual or suspicious activities using detection mechanisms such as log monitoring?	Specify if regular security monitoring and alerting is performed. If yes, does it include log monitoring for unusual or suspicious behavior?	Yes. All logs are monitored for unusual behavior such as multiple failed logins, login from an unusual geolocation, or other suspicious alerts.
	Risk Management/Incident Response 5.3.3 - Incident Detection - Third Party Data Breach	Is there a process to identify and detect and log subcontractor security, privacy, or data breach issues?	Specify if there is a process in place to identify and detect third-party vendors or subcontractors for data breach, security issues, or privacy issues.	Yes
SLA for incident notification	Risk Management/Incident Response 5.4.1 - SLA for Incident Notification (Requires manual attestation)	What is the SLA for sending notification about incidents or breaches?	What is the SLA for sending notification about incidents or breaches?	7 days

Security and configuration policy controls

Security and configuration policy controls evaluate security policies and security configurations that protect an organization's assets. This table lists the values and descriptions for security and configuration policy controls.

Control set	Control title	Control description	Evidence extraction detail	Sample value
Policies for information security	Security and Configuration Policy 10.1.1 - Policies for Information Security - Information Security Policy	Do you have an information security policy that is owned and maintaine d by a security team?	Specify if you have an information security policy. If yes, share or upload a manual evidence.	Yes. We build our security policy based on NIST framework.
	Security and Configuration Policy 10.1.2 - Policies for Information Security - Policy Review	Are all security policies reviewed annually?	Specify if security policies are reviewed annually. If no, how often are the policies reviewed?	Yes. Reviewed every year.
Policies for security configurations	Security and Configura tion Policy 10.2.1 - Policies for Security Configura tions - Security Configura tions (Requires	Are security configuration standards maintained and documented?	Specify if all security configuration standards are maintained and documented. If yes, share or upload a manual evidence.	Yes

Control set	Control title	Control description	Evidence extraction detail	Sample value
	manual attestation)			
	Security and Configuration Policy 10.2.2 - Policies for Security Configurations - Security Configurations Review (Requires manual attestation)	Are security configurations reviewed at least annually?	Specify if security configurations are reviewed at least annually. If no, specify the frequency of review.	Yes. Reviewed every 3 months.
	Security and Configuration Policy 10.2.3 - Policies for Security Configurations - Changes to Configurations	Are changes to configurations logged?	Specify if configuration changes are logged. If yes, how long are the logs retained?	Yes. All changes to configurations are monitored and logged. Alerts are raised when configurations are changed. Logs are retained for 6 months.

Exporting snapshots as a buyer using AWS Marketplace Vendor Insights

A *snapshot* is a point-in-time posture of a security profile. Exporting snapshots provides a way to download and review data offline, review evidence data, and compare products.

Export a snapshot

You can export to JSON or CSV formats. To export a snapshot, follow these steps.

1. Sign in to the AWS Management Console and open the AWS Marketplace console.
2. Choose **Vendor Insights**.
3. From **Vendor Insights**, choose a product.
4. From the **Security and compliance** tab, go to the **Summary** section, and then choose **Export**.
5. From the dropdown list, choose **Download (JSON)** or **Download (CSV)**.

Controlling access in AWS Marketplace Vendor Insights

AWS Identity and Access Management (IAM) is an AWS service that helps you control access to AWS resources. IAM is an AWS service that you can use with no additional charge. If you're an administrator, you control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS Marketplace resources. AWS Marketplace Vendor Insights uses IAM to control access to seller data, assessments, seller self-attestation, and industry standard audit reports.

The recommended way to control who can do what in AWS Marketplace Management Portal is to use IAM to create users and groups. Then you add the users to the groups, and manage the groups. You can assign a policy or permissions to the group that provide read-only permissions. If you have other users that need read-only access, you can add them to the group you created rather than adding permissions to their AWS account.

A *policy* is a document that defines the permissions that apply to a user, group, or role. The permissions determine what users can do in AWS. A policy typically allows access to specific actions, and can optionally grant that the actions are allowed for specific resources, like Amazon EC2 instances, Amazon S3 buckets, and so on. Policies can also explicitly deny access. A *permission* is a statement within a policy that allows or denies access to a particular resource.

> **Important**
>
> All of the users that you create authenticate by using their credentials. However, they use the same AWS account. Any change that a user makes can impact the whole account.

AWS Marketplace has permissions defined to control the actions that someone with those permissions can take in AWS Marketplace Management Portal. There are also policies that AWS Marketplace creates and manages that combine several permissions. The `AWSMarketplaceSellerProductsFullAccess` policy gives the user full access to products in the AWS Marketplace Management Portal.

For more information about the actions, resources, and condition keys that are available, see Actions, resources, and condition keys for AWS Marketplace Vendor Insights in the *Service Authorization Reference*.

Permissions for AWS Marketplace Vendor Insights buyers

You can use the following permissions in IAM policies for AWS Marketplace Vendor Insights. You can combine permissions into a single IAM policy to grant the permissions you want.

`GetProfileAccessTerms`

`GetProfileAccessTerms` allows users to retrieve necessary terms to review, accept, and get access to a AWS Marketplace Vendor Insights profile.

Action groups: Read-only and read-write.

Required resources: `SecurityProfile`.

`ListEntitledSecurityProfiles`

`ListEntitledSecurityProfiles` allows users to list all security profiles they have an active entitlement to read.

Action groups: Read-only, list-only, and read-write.

Required resources: None

`ListEntitledSecurityProfileSnapshots`

`ListEntitledSecurityProfileSnapshots` allows users to list the security profile snapshots for a security profile that they have an active entitlement to read.`SecurityProfile`.

Action groups: Read-only, list-only, and read-write.

Required resources: `SecurityProfile`

GetEntitledSecurityProfileSnapshot

`GetEntitledSecurityProfileSnapshot` allows users to get the details of a security profile snapshot for a security profile that they have an active entitlement to read.

Action groups: Read-only and read-write.

Required resources: `SecurityProfile`

Security on AWS Marketplace

We list software from high-quality sellers, and actively work to maintain the quality of our selection. Because every customer is different, our goal is to provide enough information about the products listed on AWS Marketplace so that customers can make good purchasing decisions.

> **Note**
>
> For information about security for data products from AWS Data Exchange, see Security in the *AWS Data Exchange User Guide*.
> For information about security for sellers on AWS Marketplace, see AWS Marketplace Security in the *AWS Marketplace Seller Guide*.

Subscriber information shared with sellers

We may share your contact information with our sellers for the following reasons:

- If it is necessary for them to provide customer training and technical support.
- For software activation, configuration, and customization of content.
- Compensate their sales teams internally.

In addition, we may share information such as company name, full address and usage fees with sellers in order for sellers to compensate their sales teams. We may also share certain information with sellers to help them evaluate the effectiveness of their marketing campaigns. Sellers may use this information along with information that they already possess to determine rewards for their sales teams or usage for a particular buyer.

Otherwise, we generally do not share customer information with sellers, and any information shared is not personally identifiable, unless you have given us permission to share such information, or we believe that providing the information to sellers is necessary to comply with laws or regulations.

Upgrade IAM policies to IPv6

AWS Marketplace customers use IAM policies to set an allowed range of IP addresses and prevent any IP addresses outside the configured range from being able to access AWS Marketplace resources.

The AWS Marketplace website domain is being upgraded to the IPv6 protocol.

IP address filtering policies that are not updated to handle IPv6 addresses might result in clients losing access to the resources on AWS Marketplace website.

Customers impacted by upgrade from IPv4 to IPv6

Customers who are using dual addressing are impacted by this upgrade. Dual addressing means that the network supports both IPv4 and IPv6.

If you are using dual addressing, you must update your IAM policies that are currently configured with IPv4 format addresses to include IPv6 format addresses.

For help with access issues, contact AWS Support.

Note

The following customers are *not* impacted by this upgrade:

- Customers who are on *only* IPv4 networks.
- Customers who are on *only* IPv6 networks.

What is IPv6?

IPv6 is the next generation IP standard intended to eventually replace IPv4. The previous version, IPv4, uses a 32-bit addressing scheme to support 4.3 billion devices. IPv6 instead uses 128-bit addressing to support approximately 340 trillion trillion trillion (or 2 to the 128th power) devices.

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

Updating an IAM policy for IPv6

IAM policies are currently used to set an allowed range of IP addresses using the `aws:SourceIp` filter.

Dual addressing supports both IPv4 and IPV6 traffic. If your network uses dual addressing, you must ensure that any IAM polices that are used for IP address filtering are updated to include IPv6 address ranges.

For example, this Amazon S3 bucket policy identifies allowed IPv4 address ranges `192.0.2.0.*` and `203.0.113.0.*` in the `Condition` element.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

To update this policy, the policy's `Condition` element is updated to include IPv6 address ranges `2001:DB8:1234:5678::/64` and `2001:cdba:3257:8593::/64`.

> **Note**
>
> DO NOT REMOVE the existing IPv4 addresses because they are needed for backward compatibility.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

For more information about managing access permissions with IAM, see Managed policies and inline policies in the *AWS Identity and Access Management User Guide*.

Testing network after update from IPv4 to IPv6

After you update your IAM policies to the IPv6 format, you can test whether your network is accessing the IPv6 endpoint and the AWS Marketplace website functionality.

Topics

- Testing network with Linux/Unix or Mac OS X
- Testing network with Windows 7 or Windows 10
- Testing the AWS Marketplace website

Testing network with Linux/Unix or Mac OS X

If you are using Linux/Unix or Mac OS X, you can test whether your network is accessing the IPv6 endpoint by using the following curl command.

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

For example, if you are connected over IPv6, the connected IP address displays the following information.

```
* About to connect() to aws.amazon.com port 443 (#0)
*   Trying IPv6 address... connected
* Connected to aws.amazon.com (IPv6 address) port 443 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1 OpenSSL/1.0.1t
 zlib/1.2.3
> Host: aws.amazon.com
```

Testing network with Windows 7 or Windows 10

If you are using Windows 7 or Windows 10, you can test whether your network can access a dual-stack endpoint over IPv6 or IPv4. Use the `ping` command as shown in the following example.

```
ping aws.amazon.com
```

This command returns IPv6 addresses if you are accessing an endpoint over IPv6.

Testing the AWS Marketplace website

Testing the AWS Marketplace website functionality after the update depends primarily on how your policy is written and what it is used for. In general, you should verify that the functionality specified in the policy works as intended.

The following scenarios can help you get started with testing the AWS Marketplace website functionality.

As a buyer on the AWS Marketplace website, test whether you can do the following tasks:

- Subscribe to an AWS Marketplace product.
- Configure an AWS Marketplace product.
- Launch or fulfill an AWS Marketplace product.

As a seller on the AWS Marketplace website, test whether you can do the following tasks:

- Manage your existing AWS Marketplace products.
- Create an AWS Marketplace product.

Controlling access to AWS Marketplace subscriptions

AWS IAM Identity Center helps you securely create or connect your workforce identities and manage their access centrally across AWS accounts and applications. IAM Identity Center is the recommended approach for workforce authentication and authorization in AWS for organizations of any size and type. For additional configuration guidance, review the AWS Security Reference Architecture.

IAM Identity Center provides a user portal where your users can find and access their assigned AWS account, roles, cloud applications, and custom applications in one place. IAM Identity Center assigns single sign-on access to users and groups in your connected directory and uses permission sets to determine their level of access. This enables temporary security credentials. You can define their level of access by assigning specific AWS managed roles for AWS Marketplace access to delegate the management of AWS Marketplace subscriptions across your AWS organization.

For example, Customer A assumes a role through federation with the `ManagedMarketplace_ViewOnly` policy attached to the role. This means Customer A can only view subscriptions in AWS Marketplace. You can create an IAM role with permissions to view subscriptions and grant permission to Customer A to assume this role.

Creating IAM roles for AWS Marketplace access

You can use IAM roles to delegate access to your AWS resources.

To create IAM roles for assigning AWS Marketplace permissions

1. Open the IAM Console.
2. In the left navigation pane, choose **Roles** and then choose **Create role**.
3. Choose your AWS account.
4. From **Add permissions**, select one of the following policies:
   - To allow permissions only to view subscriptions, but not change them, choose **AWSMarketplaceRead-only**.
   - To allow permissions to subscribe and unsubscribe, choose **AWSMarketplaceManageSubscriptions**.
   - To allow complete control of your subscriptions, choose **AWSMarketplaceFullAccess**.
5. Choose **Next**.

6. For **Role name**, enter a name for the role. For example, *MarketplaceReadOnly* or *MarketplaceFullAccess*. Then choose **Create role**. For more information, see Creating IAM roles.

> **Note**
>
> The administrator of the specified account can grant permission to assume this role to any user in that account.

Repeat the preceding steps to create more roles with different permission sets so that each user persona can use the IAM role with customized permissions.

You're not limited to the permissions in the AWS managed policies that are described here. You can use IAM to create policies with custom permissions and then add those policies to IAM roles. For more information, see Managing IAM policies and Adding IAM identity permissions.

AWS managed policies for AWS Marketplace

You can use AWS managed policies to provide basic AWS Marketplace permissions. Then, for any unique scenarios, you can create your own policies and apply them to the roles with the specific requirements for your scenario. The following basic AWS Marketplace managed policies are available to you to control who has which permissions:

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

AWS Marketplace also provides specialized managed policies for specific scenarios. For a full list of AWS managed policies for AWS Marketplace buyers, as well as descriptions of what permissions they provide, see AWS managed policies for AWS Marketplace buyers.

Permissions for working with License Manager

AWS Marketplace integrates with AWS License Manager to manage and share licenses for products that you subscribe to between accounts in your organization. To view the full details of your subscriptions in AWS Marketplace, a user must be able to list license information from AWS License Manager.

To make sure that your users have the permissions they need to see all the data about their AWS Marketplace products and subscriptions, add the following permission:

- `license-manager:ListReceivedLicenses`

For more information about setting permissions, see Managing IAM policies in the *IAM User Guide*.

Additional resources

For more information about managing IAM roles, see IAM Identities (users, user groups, and roles) in the *IAM User Guide*.

For more information about managing IAM permissions and policies, see Controlling access to AWS resources using policies in the *IAM User Guide*.

For more information about managing IAM permissions and policies for data products in AWS Data Exchange, see Identity and access management in AWS Data Exchange in the *AWS Data Exchange User Guide*.

AWS managed policies for AWS Marketplace buyers

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*.

This section lists each of the policies used to manage buyer access to AWS Marketplace. For information about seller policies, see AWS managed policies for AWS Marketplace sellers in the *AWS Marketplace Seller Guide*.

Topics

AWS managed policy: AWSMarketplaceDeploymentServiceRolePolicy

You can't attach `AWSMarketplaceDeploymentServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role that allows AWS Marketplace to perform actions on your behalf. For more information, see Using service-linked roles for AWS Marketplace.

This policy grants contributor permissions that allow AWS Marketplace to manage deployment-related parameters, which are stored as secrets in AWS Secrets Manager, on your behalf.

AWS managed policy: AWSMarketplaceFullAccess

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

This policy grants administrative permissions that allow full access to AWS Marketplace and related services, both as a buyer and a seller. These permissions include the ability to subscribe and unsubscribe to AWS Marketplace software, manage AWS Marketplace software instances from the AWS Marketplace, creating and managing private marketplace in your account, as well as access to Amazon EC2, AWS CloudFormation, and Amazon EC2 Systems Manager.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:*",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks",
                "cloudformation:List*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CopyImage",
                "ec2:DeregisterImage",
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:DescribeInstanceStatus",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:CreateTopic",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:setTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*image-build*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
```

```
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        }
    ]
}
```

AWS managed policy: AWSMarketplaceLicenseManagementServiceRolePolicy

You can't attach AWSMarketplaceLicenseManagementServiceRolePolicy to your IAM entities. This policy is attached to a service-linked role that allows AWS Marketplace to perform actions on your behalf. For more information, see Using service-linked roles for AWS Marketplace.

This policy grants contributor permissions that allow AWS Marketplace to manage licenses on your behalf.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLicenseManagerActions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "license-manager:ListReceivedGrants",
                "license-manager:ListDistributedGrants",
                "license-manager:GetGrant",
                "license-manager:CreateGrant",
                "license-manager:CreateGrantVersion",
                "license-manager:DeleteGrant",
                "license-manager:AcceptGrant"
            ],
            "Resource": [
                "*"
            ]
```

```
        }
    ]
}
```

AWS managed policy: AWSMarketplaceManageSubscriptions

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

This policy grants contributor permissions that allow subscribing and unsubscribing to AWS Marketplace products.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "aws-marketplace:Subscribe",
                "aws-marketplace:Unsubscribe"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWS managed policy: AWSMarketplaceProcurementSystemAdminFullAccess

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

This policy grants admin permissions that allow managing all aspects of an AWS Marketplace eProcurement integration, including listing the accounts in your organization. For more information about eProcurement integrations, see Integrating AWS Marketplace with procurement systems .

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:PutProcurementSystemConfiguration",
                "aws-marketplace:DescribeProcurementSystemConfiguration",
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS managed policy: AWSMarketplaceRead-only

You can attach the `AWSMarketplaceRead-only` policy to your IAM identities.

This policy grants read-only permissions that allows viewing products, private offers, and subscriptions for your account on AWS Marketplace, as well as viewing the Amazon EC2, AWS Identity and Access Management, and Amazon SNS resources in the account.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:DescribeBuilds",
                "iam:ListRoles",
                "iam:ListInstanceProfiles",
                "sns:GetTopicAttributes",
                "sns:ListTopics"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
```

```
            ]
        }
    ]
}
```

AWS managed policy: AWSPrivateMarketplaceAdminFullAccess

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

This policy grants administrator permissions that allow full access to manage private marketplaces in your account (or organization). For more information about using multiple administrators, see the section called “Creating custom policies for private marketplace administrators”.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceRequestPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:StartChangeSet",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "PrivateMarketplaceCatalogTaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:TagResource",
                "aws-marketplace:UntagResource",
                "aws-marketplace:ListTagsForResource"
            ],
            "Resource": "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AWSPrivateMarketplaceRequests

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

This policy grants contributor permissions that allow access to request products be added to your private marketplace, and to view those requests. These requests must be approved or denied by a private marketplace administrator.

Permissions details

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AWSServiceRoleForPrivateMarketplaceAdminPolicy

You can't attach `AWSServiceRoleForPrivateMarketplaceAdminPolicy` to your IAM entities. This policy is attached to a service-linked role that allows AWS Marketplace to perform actions on your behalf. For more information, see Using service-linked roles for AWS Marketplace.

This policy grants contributor permissions that allow AWS Marketplace to describe and update Private Marketplace resources and describe AWS Organizations.

AWS managed policy: AWSVendorInsightsAssessorFullAccess

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

This policy grants full access for viewing entitled AWS Marketplace Vendor Insights resources and managing AWS Marketplace Vendor Insights subscriptions. These requests must be approved or denied by an administrator. It allows read-only access to AWS Artifact third-party reports.

AWS Marketplace Vendor Insights identifies assessor is equal to buyer and vendor is equal to seller.

Permissions details

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

```
      "Action": [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:AgreementType": "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

AWS managed policy: AWSVendorInsightsAssessorReadOnly

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

This policy grants read-only access for viewing entitled AWS Marketplace Vendor Insights resources. These requests must be approved or denied by an administrator. It allows read-only access to reports in AWS Artifact.

requests must be approved or denied by an administrator. It allows read-only access to AWS Artifact third-party reports.

AWS Marketplace Vendor Insights identifies assessor as the buyer and vendor is equal to the seller for the purposes of this guide.

Permissions details

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

AWS Marketplace updates to AWS managed policies

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

Change	Description	Date
Removed the legacy `AWSMarketplaceImageBuildFullAccess` AWS Marketplace policy	AWS Marketplace discontinued the Private Image Build delivery method, so the `AWSMarketplaceImageBuildFullAcces` policy was also discontinued.	May 30, 2024
AWSServiceRoleForPrivateMarketplaceAdminPolicy – Added policy for new feature in AWS Marketplace	AWS Marketplace added a new policy to support managing Private Marketplace resources and describing AWS Organizations.	February 16, 2024
AWSPrivateMarketplaceAdminFullAccess – Update to existing policy	AWS Marketplace updated the policy to support reading AWS Organizations data.	February 16, 2024
AWSMarketplaceDeploymentServiceRolePolicy – Added policy for new feature in AWS Marketplace	AWS Marketplace added a new policy to support managing deployment-related parameters.	November 29, 2023
AWSMarketplaceRead-only and AWSMarketplaceManageSubscriptions – updates to existing policies	AWS Marketplace updated existing policies to allow access to the **Private offers** page.	January 19, 2023
AWSPrivateMarketplaceAdminFullAccess – Update to existing policy	AWS Marketplace updated the policy for the new tag-based authorization feature.	December 9, 2022
AWSVendorInsightsAssessorReadOnly AWS Marketplace updated `AWSVendorInsightsAssessorReadOnly`	AWS Marketplace updated `AWSVendorInsightsAssessorReadOnly` to add read-only access to reports	November 30, 2022

Change	Description	Date
	in AWS Artifact third-party report (preview).	
AWSVendorInsightsAssessorFullAccess AWS Marketplace updated `AWSVendorInsightsAssessorFullAccess`	AWS Marketplace updated `AWSVendorInsightsAssessorFullAccess` to add agreement search and read-only access to AWS Artifact third-party report (preview).	November 30, 2022
AWSVendorInsightsAssessorFullAccess and AWSVendorInsightsAssessorReadOnly – Added policies for new feature in AWS Marketplace	AWS Marketplace added policies for the new feature AWS Marketplace Vendor Insights: `AWSVendorInsightsAssessorFullAccess` and `AWSVendorInsightsAssessorReadOnly`	July 26, 2022
AWSMarketplaceFullAccess and AWSMarketplaceImageBuildFullAccess – Updates to an existing policies	AWS Marketplace removed no longer needed permissions to improve security.	March 4, 2022
AWSPrivateMarketplaceAdminFullAccess – Update to an existing policy	AWS Marketplace removed unused permissions in the `AWSPrivateMarketplaceAdminFullAccess` policy.	August 27, 2021

Change	Description	Date
AWSMarketplaceFullAccess – Update to an existing policy	AWS Marketplace removed a duplicate `ec2:DescribeAccountAttributes` permission from `AWSMarketplaceFullAccess` policy.	July 20, 2021
AWS Marketplace started tracking changes	AWS Marketplace started tracking changes for its AWS managed policies.	April 20, 2021

Finding your AWS account number for customer support

If you or your users need to contact AWS Support, you need your AWS account number.

To find your AWS account number

1. Sign in to the AWS Management Console with your user name.
2. In the top navigation bar, choose **Support** and then choose **Support Center**.

Your AWS account ID (account number) appears below the top navigation bar.

Using service-linked roles for AWS Marketplace

AWS Marketplace 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 Marketplace. Service-linked roles are predefined by AWS Marketplace and include all the permissions that the service requires to call other AWS services on your behalf.

Topics

- Using roles to share entitlements for AWS Marketplace
- Using roles to work with purchase orders in AWS Marketplace
- Using roles to configure and launch products in AWS Marketplace
- Using roles to configure Private Marketplace in AWS Marketplace

Using roles to share entitlements for AWS Marketplace

AWS Marketplace 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 Marketplace. Service-linked roles are predefined by AWS Marketplace 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 Marketplace easier because you don't have to add the necessary permissions manually. AWS Marketplace defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Marketplace can assume its roles. The defined permissions include the trust policy and the permissions policy. That permissions policy can't be attached to any other IAM entity.

To share your AWS Marketplace subscriptions to other accounts in your AWS organization with AWS License Manager, you must give AWS Marketplace permissions for each account you want to share with. Do this by using the **AWSServiceRoleForMarketplaceLicenseManagement** role. See Creating a service-linked role for AWS Marketplace for more details.

For information about other services that support service-linked roles, see AWS services that work with IAM, and look for the services with **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 Marketplace

AWS Marketplace uses the service-linked role named **AWSServiceRoleForMarketplaceLicenseManagement**. This role provides AWS Marketplace with permissions to create and manage licenses in AWS License Manager for the products that you subscribe to in AWS Marketplace.

The **AWSServiceRoleForMarketplaceLicenseManagement** service-linked role trusts the following service to perform actions in License Manager on your behalf:

- `license-management.marketplace.amazonaws.com`

The role permissions policy named **AWSMarketplaceLicenseManagementServiceRolePolicy** allows AWS Marketplace to complete the following actions on the specified resources:

- Actions:
  - `"organizations:DescribeOrganization"`

- `"license-manager:ListReceivedGrants"`
- `"license-manager:ListDistributedGrants"`
- `"license-manager:GetGrant"`
- `"license-manager:CreateGrant"`
- `"license-manager:CreateGrantVersion"`
- `"license-manager:DeleteGrant"`
- `"license-manager:AcceptGrant"`

- Resources:
  - All resources (`"*"`)

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Marketplace

AWS Marketplace creates the service-linked role for you when you set up integration with AWS License Manager.

You can specify that AWS Marketplace create the service-linked role for all accounts in your organization at once, or you can create the service-linked role for one account at a time. The option to create service-linked roles across all accounts is only available if your organization has **All features** enabled. For more details, see Enabling all features in your organization in the *AWS Organizations User Guide*.

To create service-linked roles across all accounts

1. In AWS Marketplace console, sign in and choose **Settings**.
2. In the **AWS Organizations integration** section, select **Create integration**.
3. On the **Create AWS Organizations integration** page, select **Enable trusted access across your organization**, then choose **Create integration**.

> **Note**
>
> This setting enables trust within AWS Organizations. As a result, in addition to the current action, future accounts that are added to the organization have the service-linked role added automatically.

To create service-linked roles for the current account

1. In AWS Marketplace console, sign in and choose **Settings**.
2. In the **AWS Organizations integration** section, select **Configure integration**.
3. On the **Create AWS Organizations integration** page, select **AWS Marketplace license management service-linked role for this Account**, then choose **Create integration**.

> **Important**
>
> If you choose to create the service-linked role only for the current account, it does not enable trusted access across your organization. You must repeat these steps for each account that wants to share (giving or receiving) licenses in AWS Marketplace. This includes accounts that are added to the organization in the future.

Editing a service-linked role for AWS Marketplace

AWS Marketplace doesn't allow you to edit the 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 Marketplace

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 Marketplace 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 manually delete the service-linked role using IAM

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

Supported Regions for AWS Marketplace service-linked roles

AWS Marketplace supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS Marketplace Regions and Endpoints.

Using roles to work with purchase orders in AWS Marketplace

AWS Marketplace 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 Marketplace. Service-linked roles are predefined by AWS Marketplace 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 Marketplace easier because you don't have to manually add the necessary permissions. AWS Marketplace defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Marketplace 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 their related resources. This protects your AWS Marketplace 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 Marketplace

AWS Marketplace uses the service-linked role named **AWSServiceRoleForMarketplacePurchaseOrders** – this role provides AWS Marketplace permissions to attach purchase order numbers to your AWS Marketplace subscriptions in AWS Billing and Cost Management.

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

- `purchase-orders.marketplace.amazonaws.com`

The role permissions policy named **AWSMarketplacePurchaseOrdersServiceRolePolicy** allows AWS Marketplace to complete the following actions on the specified resources:

- Action: `"purchase-orders:ViewPurchaseOrders", "purchase-orders:ModifyPurchaseOrders"` on `"*"`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Marketplace

You don't need to manually create a service-linked role. When you set up integrating with AWS Billing and Cost Management, AWS Marketplace creates the service-linked role for you.

> **Note**
>
> Within AWS Organizations, this setting only works in the management account. You must perform this procedure from the management account. This sets up the service linked role and purchase order support for all accounts in the organization.

To create a service-linked role

1. In the AWS Marketplace console, sign in to the management account and choose **Settings**.
2. In the **AWS Billing integration** section, select **Configure integration**.

3. On the **Create AWS Billing integration** page, select **AWS Marketplace billing management service-linked role for your organization**, then choose **Create integration**.

If you delete this service-linked role, and then need to create it again, you can use the same process to re-create the role in your account. When you set up integrating with AWS Billing and Cost Management, AWS Marketplace creates the service-linked role for you again.

Editing a service-linked role for AWS Marketplace

AWS Marketplace does not allow you to edit the **AWSServiceRoleForMarketplacePurchaseOrders** 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 Marketplace

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 your service-linked role before you can manually delete it.

Manually deleting the service-linked role

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

Supported Regions for AWS Marketplace service-linked roles

AWS Marketplace supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS Marketplace Regions and Endpoints.

Using roles to configure and launch products in AWS Marketplace

AWS Marketplace 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 Marketplace. Service-linked roles are predefined by AWS Marketplace 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 Marketplace easier because you don't have to manually add the necessary permissions. AWS Marketplace defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Marketplace 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.

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 Marketplace

AWS Marketplace uses the service-linked role named **AWSServiceRoleForMarketplaceDeployment** to allow AWS Marketplace to manage deployment-related parameters, which are stored as secrets in AWS Secrets Manager, on your behalf. These secrets can be referenced by sellers in AWS CloudFormation templates, which you can launch when configuring products that have Quick Launch enabled in AWS Marketplace.

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

- `deployment.marketplace.amazonaws.com`

Use the role permissions policy named **AWSMarketplaceDeploymentServiceRolePolicy** to allow AWS Marketplace to complete the actions on your resources.

> **Note**
>
> For more information about AWS Marketplace managed policies, see AWS managed policies for AWS Marketplace buyers.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ManageMarketplaceDeploymentSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:CreateSecret",
```

```
    "secretsmanager:PutSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:DeleteSecret",
    "secretsmanager:RemoveRegionsFromReplication"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "ListSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:ListSecrets"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "TagMarketplaceDeploymentSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:TagResource"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
   "Condition": {
    "Null": {
     "aws:RequestTag/expirationDate": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": [
      "expirationDate"
     ]
    },
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
```

```
  }
 ]
}
```

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Marketplace

Setting up the service-linked role is a one-time action that provides the permissions for all products that have Quick Launch enabled, as long as the role exists.

When you configure a product that has Quick Launch enabled, AWS Marketplace will detect whether you have the required service-linked role created for your account. If the role is missing, a prompt to enable AWS Marketplace deployment parameters integration displays, which includes an **Enable integration** button. AWS Marketplace creates the service-linked role for you when you select this button.

> **Important**
>
> This service-linked role will appear in your account if you've previously configured a product that has Quick Launch enabled. For more information, see A new role appeared in my AWS account.

If you delete this service-linked role and need to create it again, you can use the same process to re-create the role in your account. When you open the **Configuration** page for any product that has Quick Launch enabled, you'll see the **Enable integration** button, which you can choose again to re-create the service-linked role.

You can also use the IAM console to create a service-linked role with the **AWS Marketplace - Deployment Management** use case. In the AWS CLI or the AWS API, create a service-linked role with the `deployment.marketplace.amazonaws.com` service name. For more information, see Creating a service-linked role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for AWS Marketplace

AWS Marketplace does not allow you to edit the 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 Marketplace

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 service is using the role when you try to delete it, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete AWS Marketplace resources used by the `deployment.marketplace.amazonaws.com` service, you must delete all Marketplace Deployment-related secrets from SecretsManager. You can find the relevant secrets by:

- Searching for secrets that are managed by `marketplace-deployment`.
- Searching for secrets with the tag key `aws:secretsmanager:owningService` and value `marketplace-deployment`.
- Searching for secrets where the secret name is prefixed with `marketplace-deployment!`.

To delete the service-linked role using IAM

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

Supported Regions for AWS Marketplace service-linked roles

AWS Marketplace supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Marketplace Regions and Endpoints.

Using roles to configure Private Marketplace in AWS Marketplace

AWS Marketplace 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 Marketplace. Service-linked roles are predefined by AWS Marketplace 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 Marketplace easier because you don't have to manually add the necessary permissions. AWS Marketplace defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Marketplace 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.

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 Marketplace

AWS Marketplace uses the service-linked role named **AWSServiceRoleForPrivateMarketplaceAdmin** to describe and update Private Marketplace resources and describe AWS Organizations.

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

- `private-marketplace.marketplace.amazonaws.com`

Use the role permissions policy named **AWSServiceRoleForPrivateMarketplaceAdminPolicy** to allow AWS Marketplace to perform the following actions on specified resources.

> **Note**
>
> For more information about AWS Marketplace managed policies, see AWS managed policies for AWS Marketplace buyers.

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

```
    "Statement": [
        {
            "Sid": "PrivateMarketplaceCatalogDescribePermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogListPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceStartChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AssociateAudience",
                        "DisassociateAudience"
                    ]
                }
```

```
            },
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Marketplace

You don't need to manually create the service-linked role. When you enable Private Marketplace for your organization, AWS Marketplace creates the service-linked role for you.

> **Note**
>
> This role is required only in the management account of AWS Organizations and is created only in the management account.

To create a service-linked role

1. On the **Getting started with Private Marketplace** page, select the options to enable trusted access across your organization and create a Private Marketplace service-linked role. These options are only available to the management account.

2. Choose **Enable Private Marketplace**.

If you're an existing Private Marketplace customer, the options to enable trusted access across your organization and enable a Private Marketplace service-linked role will be available on the Settings page of your private marketplace administrative dashboard.

If you delete this service-linked role and need to create it again, you can use the same process to re-create the role in your account.

Editing a service-linked role for AWS Marketplace

AWS Marketplace doesn't allow you to edit the service-linked role. After you create a service-linked role, you can't 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 Marketplace

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.

Before you can delete the service-linked role, you must:

- Disable trusted access across your organization.
- Disassociate all private marketplace experiences.

To manually delete the service-linked role using IAM

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

Supported Regions for AWS Marketplace service-linked roles

AWS Marketplace supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Marketplace Regions and Endpoints.

Creating a private marketplace administrator

You can create an administrators group to manage your company's private marketplace settings. After private marketplace is enabled for your organization, administrators for the private marketplace can perform many tasks including the following:

- View and create experiences and audiences.
- Add products to private marketplace experiences.
- Remove products from private marketplace experiences.
- Configure the user interface of private marketplace experiences.
- Enable and disable private marketplace experiences.
- Call the AWS Marketplace Catalog API to manage private marketplace experiences programmatically.

To create multiple private marketplace administrators where each administrator is limited to a subset of tasks, see the section called "Creating custom policies for private marketplace administrators".

> **Note**
>
> Enabling private marketplace is a one-time action that must happen from the management account. For more information, see Getting started with private marketplace.

You grant AWS Identity and Access Management (IAM) permissions to administer your private marketplace by attaching the the section called "AWSPrivateMarketplaceAdminFullAccess" to a user, group, or role. We recommend using a group or role. For more information about how to attach the policy, see Attaching a policy to a user group in the *IAM User Guide*.

For more information about the permissions in the `AWSPrivateMarketplaceAdminFullAccess` policy, see the section called "AWSPrivateMarketplaceAdminFullAccess". To learn about other policies for use in AWS Marketplace, sign in to the AWS Management Console, and go to the IAM policies page. In the search box, enter **`Marketplace`** to find all of the policies that are associated with AWS Marketplace.

Creating custom policies for private marketplace administrators

Your organization can create multiple private marketplace administrators where each administrator is limited to a subset of tasks. You can tune AWS Identity and Access Management (IAM) policies to specify condition keys and resources on AWS Marketplace Catalog API actions listed in Actions, resources, and condition keys for AWS Marketplace Catalog. The general mechanism to use AWS Marketplace Catalog API change types and resources to tune IAM policies is described in the AWS Marketplace Catalog API guide. For a list of all change types available in the private AWS Marketplace, see Working with a private marketplace.

To create customer managed policies, see Creating IAM policies. Following is an example policy JSON that you can use to create an administrator who can only add or remove products from private marketplaces.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AllowProductProcurement",
                        "DenyProductProcurement"
                    ]
                }
            },
            "Resource": "*"
        }
    ]
}
```

A policy can also be limited to manage a subset of private marketplace resources. Following is an example policy JSON you can use to create an administrator who can only manage a specific private marketplace experience. This example uses a resource string with `exp-1234example` as the `Experience` identifier.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
```

```
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/exp-1234example"
            ]
        }
    ]
}
```

For details about how entity identifiers can be retrieved and to view the set of private marketplace resources, see Working with a private marketplace.

Document history

The following table describes the documentation for this release of the *AWS Marketplace Buyer Guide*.

For notification about updates to this documentation, you can subscribe to the RSS feed.

Change	Description	Date
Updated Amazon Machine Image (AMI) annual agreement amendment options	Buyers can now amend their subscription to add or switch AMI instance types.	May 30, 2024
Removed the AWSMarketplaceImageBuildFullAccess policy	AWS Marketplace discontinued the Private Image Build delivery method, so the `AWSMarketplaceImageBuildFullAcces` policy was also discontinued.	May 30, 2024
New demo and private offer options on AWS Marketplace	AWS Marketplace now supports demo and private offer request options on product detail pages for select products.	April 1, 2024
Updated policy for AWS Organizations support	Updated managed policy `AWSPrivateMarketplaceAdminFullAccess` to allow access to read AWS Organizations data.	February 16, 2024
New service-linked role for products in AWS Marketplace	AWS Marketplace now provides a service-linked role to describe and update Private Marketplace resources	February 16, 2024

	and describe AWS Organizations.	
New private marketplace experience on AWS Marketplace	AWS Marketplace now supports an integration with AWS Organizations and the ability to register delegated administrators to administrate private marketplace experiences.	February 16, 2024
General availability for future dated agreements in AWS Marketplace	Future dated agreements functionality for all SaaS ISVs and Channel Partners is now generally available in AWS Marketplace. Using future dated agreements, customers can pre-book deals or set up renewals when they have existing purchases on the same product listing with decreased operational effort.	January 16, 2024
Support for the Canada West (Calgary) Region	AWS Marketplace now supports the following AWS Region: Canada West (Calgary).	December 20, 2023
New service-linked role for products in AWS Marketplace	AWS Marketplace now provides a service-linked role to manage deployment-related parameters, which are stored as secrets in AWS Secrets Manager, on behalf of buyers.	November 29, 2023

New Quick Launch deployment option for buyers	Buyers can now reduce the time, resources, and steps required to configure, deploy, and launch applicabl e software as a service (SaaS) products in AWS Marketplace.	November 29, 2023
Flexible payment schedules are available for private offers	Flexible Payment Schedules (FPS) for private offers are now available to all customers in the AWS Marketplace.	November 17, 2023
Third-party add-ons from Amazon EKS	Customers can now subscribe to third-party add-ons from the Amazon EKS console without being redirected to AWS Marketplace.	October 18, 2023
Support for Amazon EventBridge	AWS Marketplace is now integrated with Amazon EventBridge, formerly called Amazon CloudWatch Events.	September 6, 2023
Support for the Israel (Tel Aviv) Region	AWS Marketplace now supports the following AWS Region: Israel (Tel Aviv).	August 1, 2023
Purchase order support for AMI annual contracts	AWS Marketplace now supports purchase order functionality for Amazon Machine Image (AMI) annual contracts.	June 29, 2023

Purchase order availability in AWS Billing console	Buyers can now manage all their purchase orders in the AWS Billing console and easily reconcile their out-of-cycle SaaS contract PDF invoices with the correspon ding purchase orders.	February 3, 2023
Support for the Asia Pacific (Melbourne) Region	AWS Marketplace now supports the following AWS Region: Asia Pacific (Melbourn e).	January 24, 2023
Updated policies for private offers page	Updated managed policies `AWSMarketplaceRead -only` and `AWSMarket placeManageSubscri ptions` to allow access to the **Private offers** page.	January 19, 2023
Private offers page	Authenticated buyers can now view the AWS Marketpla ce private offers extended to their AWS account on the **Private offers** page.	January 19, 2023
Updated email notifications for buyers	Buyers are now notified when a private offer is published.	December 22, 2022
SaaS free trials for subscript ions are now available to buyers on AWS Marketplace	Buyers can now subscribe to free trials for subscription SaaS products.	December 16, 2022

Buyers can accept a SaaS private offer upgrade or renewal	If a seller has upgraded or renewed a previous SaaS private offer, buyers can accept a new private offer without having to cancel their existing agreement.	December 13, 2022
AWS Marketplace supports archiving private marketplace experiences	Buyers can now archive and reactivate private marketplace experiences in AWS Marketplace.	December 12, 2022
Updated policy for AWS Marketplace tag-based authorization feature	Updated the `AWSPrivateMarketplaceAdminFullAccess` policy to support tag-based authorization in AWS Marketplace.	December 9, 2022
Added new topic providing information on how to cancel your subscription	Added information on how to cancel your subscription to AMI, ML, and SaaS products in AWS Marketplace. Also, added information on canceling your auto-renewal for a SaaS contract.	December 8, 2022
Updated policies for buyers in AWS Marketplace Vendor Insights	Updated managed policies `AWSVendorInsightsAssessorFullAccess` and `AWSVendorInsightsAssessorReadOnly` for AWS Marketplace Vendor Insights buyers.	November 30, 2022

Controlling access for buyers in AWS Marketplace Vendor Insights	Added a new topic in AWS Marketplace Vendor Insights to describe actions and permissions available to buyers.	November 30, 2022
Support for Asia Pacific (Hyderabad) Region	AWS Marketplace now supports the following AWS Region: Asia Pacific (Hyderabad).	November 22, 2022
Support for Europe (Spain) Region	AWS Marketplace now supports the following AWS Region: Europe (Spain).	November 16, 2022
Support for Europe (Zurich) Region	AWS Marketplace now supports the following AWS Region: Europe (Zurich).	November 9, 2022
AWS Marketplace website upgrade to IPv6 by December 2022	Buyers who currently use the IPv4 format address in their IAM policies are advised to update their IAM policies to IPv6 format addresses before December 15, 2022.	September 29, 2022
AWS Marketplace Private marketplace granular permissions	Buyers now have more granular permissions to manage private marketplace experiences.	September 8, 2022

Added two policies for AWS Marketplace Vendor Insights.	Added two policies `AWSVendorInsightsAssessorFullAccess` and `AWSVendorInsightsAssessorReadOnly` for AWS Marketplace Vendor Insights a feature offering software risk assessment	July 26, 2022
AWS Marketplace Vendor Insights	AWS Marketplace Vendor Insights is a feature offering software risk assessment.	July 26, 2022
Payment methods update	Documentation-only update to clarify how to change payment methods in the AWS Billing console.	June 1, 2022
SaaS free trials for contracts	Buyers can now subscribe to SaaS free trials for contracts to explore products before transitioning into paid trials.	May 31, 2022
Vendor-metering tags added for AMI, Container, and SaaS products	New feature providing tags to help customers understand their AWS Marketplace resource usage across vendor-provided metrics.	May 27, 2022
Email notifications added to buyer transactions	New feature enabling email notifications to buyer verifying agreements made in AWS Marketplace.	May 23, 2022

Auto approval of Free/BYOL products for eProcurement customers enabled	Customers can use products immediately with the new automatic approval of free/BYOL products for eProcurement customers.	May 2, 2022
Contract modifications enabled for buyers in AMI and Container Product contracts	AMI and Container product contracts can be modified to purchase additional entitlements or and enable the automatic subscription renewal option.	April 6, 2022
Ability to track license usage	Buyers can now track usage based license metrics for AMI and SaaS products with AWS License Manager.	March 28, 2022
Updates to Helm CLI version	Updated container products documentation regarding the Helm CLI version change from 3.7.0 to 3.7.1. This is the only compatible version at this time.	March 8, 2022
Updates to existing managed policies	Permissions that were no longer needed were removed from the following policies: `AWSMarketplaceFullAccess` and `AWSMarketplaceImageBuildFullAccess`.	March 4, 2022

Ability for EMEA-based buyers to purchase products through Amazon Web Services EMEA SARL	AWS Marketplace buyers whose AWS accounts are based in countries and territories in Europe, the Middle East, and Africa (EMEA), excluding Turkey and South Africa, can now receive AWS Marketplace invoices through Amazon Web Services EMEA SARL for purchases from EMEA-eligible sellers.	January 7, 2022
Support for Asia Pacific (Jakarta) Region	AWS Marketplace now supports the following AWS Region: Asia Pacific (Jakarta).	December 13, 2021
Helm chart delivery method for container-based products	Buyers can now launch container-based products by installing a Helm chart in their launch environments.	November 29, 2021
General updates and reorganization of container-based product documentation	Updated container-based product documentation to add more information and clarity around finding, subscribing to, and launching container-based products.	November 29, 2021

Added documentation for QuickLaunch	Buyers can now use QuickLaunch when launching container-based products with a Helm chart delivery method. QuickLaunch is a feature in AWS Marketplace that leverages AWS CloudFormation to quickly create a new Amazon EKS cluster and launch a container-based application on it.	November 29, 2021
Contract pricing for AMI-based products and container-based products	Buyers are now able to purchase an AMI-based product or a Container-based product with upfront pricing.	November 17, 2021
Support for purchase orders in SaaS products	AWS Marketplace supports adding purchase order numbers to purchases of software as a service (SaaS) contracts.	October 28, 2021
Support for SAP Ariba integration	AWS Marketplace supports integration with the SAP Ariba procurement system.	October 13, 2021
Support for AMI aliases	AWS Marketplace supports using aliases for AMI IDs that can be used across regions.	September 8, 2021
Removed unused permissions in managed policy	Unused permissions from `AWSPrivateMarketplaceAdminFullAccess` AWS managed policy have been removed.	August 27, 2021

Support for sharing licenses through AWS License Manager	You can share licenses to products that you purchase with other accounts in your AWS organization.	December 3, 2020
AWS Marketplace supports professional services offerings	AWS Marketplace now supports purchasing professio nal services.	December 3, 2020
Support for preferred currency	You can pay for AWS Marketplace purchases using your preferred currency.	July 27, 2020
You can review and accept private offer upgrades and renewals	Sellers can provide upgrade and renewal private offers for SaaS contract and SaaS contract with consumpti on products that you can review and accept while on an existing agreement.	May 28, 2020
AWS Marketplace supports data products through AWS Data Exchange	You can now subscribe to AWS Data Exchange data products in AWS Marketplace.	November 13, 2019
AWS Marketplace supports paid hourly containers	AWS Marketplace now supports paid hourly containers running on Amazon Elastic Kubernetes Service (Amazon EKS).	September 25, 2019
Updated private offers on AWS Marketplace	Updated content to provide more information on accepting different types of private offers.	March 29, 2019

Updated Security on AWS Marketplace	Updated IAM policies information, restructured section for readability.	March 25, 2019
Added content for the private marketplace feature	Added content supporting the release of *Private Marketplace*.	November 27, 2018
Initial release of the user guide for buyers	Initial release of the *AWS Marketplace Buyer Guide*.	November 16, 2018

AWS Glossary

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