AWS License Manager

User Guide

AWS License Manager: User Guide

Table of Contents

What is AWS License Manager?

AWS License Manager is a service that makes it easier for you to manage your software licenses from software vendors (for example, Microsoft, SAP, Oracle, and IBM) centrally across AWS and your on-premises environments. This provides control and visibility into the usage of your licenses, enabling you to limit licensing overages and reduce the risk of non-compliance and misreporting.

As you build out your cloud infrastructure on AWS, you can save costs by using bring-your-own-license (BYOL) opportunities. That is, you can re-purpose your existing license inventory for use with your cloud resources.

License Manager reduces the risk of licensing overages and penalties with inventory tracking that is tied directly into AWS services. With rule-based controls on the consumption of licenses, administrators can set hard or soft limits on new and existing cloud deployments. Based on these limits, License Manager helps stop non-compliant server usage before it happens.

License Manager's built-in dashboards provide ongoing visibility into license usage and assistance with vendor audits.

License Manager supports tracking any software that is licensed based on virtual cores (vCPUs), physical cores, sockets, or number of machines. This includes a variety of software products from Microsoft, IBM, SAP, Oracle, and other vendors.

With AWS License Manager, you can centrally track licenses and enforce limits across multiple Regions, by maintaining a count of all the checked out entitlements. License Manager also tracks the end-user identity and the underlying resource identifier, if available, associated with each check out, along with the check-out time. This time-series data can be tracked to the ISV through CloudWatch metrics and events. ISVs can use this data for analytics, auditing, and other similar purposes.

AWS License Manager is integrated with AWS Marketplace and AWS Data Exchange, and with the following AWS services: AWS Identity and Access Management (IAM), AWS Organizations, Service Quotas, AWS CloudFormation, AWS resource tagging, and AWS X-Ray.

Managed Entitlements

With License Manager, a license administrator can distribute, activate, and track software licenses across accounts and throughout an organization.

Independent software vendors (ISVs) can use AWS License Manager to manage and distribute software licenses and data to end users by means of managed entitlements. As an issuer, you can track the usage of your seller-issued licenses centrally using the License Manager dashboard. ISVs selling through AWS Marketplace benefit from automatic license creation and distribution as a part of the transaction workflow. ISVs can also use License Manager to create license keys and activate licenses for customers without an AWS account.

License Manager uses open, secure, industry standards for representing licenses and allows customers to cryptographically verify their authenticity. License Manager supports a variety of different licensing models including perpetual licenses, floating licenses, subscription licenses, and usage-based licenses. If you have licenses that must be node-locked, License Manager provides mechanisms to consume your licenses in that way.

You can create licenses in AWS License Manager and distribute them to end users using an IAM identity or through digitally signed tokens generated by AWS License Manager. End-users using AWS can further

redistribute the license entitlements to AWS identities in their respective organizations. End users with distributed entitlements can check out and check in the required entitlements from that license through your software integration with AWS License Manager. Each license check out specifies the entitlements, the associated quantity, and check-out time period such as checking out 10 **`admin-users`** for 1 hour. This check out can be performed based on the underlying IAM identity for the distributed license or based on the long-lived tokens generated by AWS License Manager through the AWS License Manager service.

Related Services

License Manager is integrated with Amazon EC2, allowing you to track licenses for the following resources:

- EC2 instances
- Dedicated Instances
- Dedicated Hosts
- Spot Instances and Spot Fleet
- Systems Manager Managed Instances

License Manager is integrated with Amazon RDS, allowing you to monitor your Oracle license usage on Amazon RDS. For more information, see Oracle Licensing in the *Amazon RDS User Guide*.

Using License Manager along with AWS Systems Manager, you can manage licenses on physical or virtual servers hosted outside of AWS.

You can use License Manager to track BYOL software obtained from the AWS Marketplace.

You can use License Manager with AWS Organizations to manage all of your organizational accounts centrally.

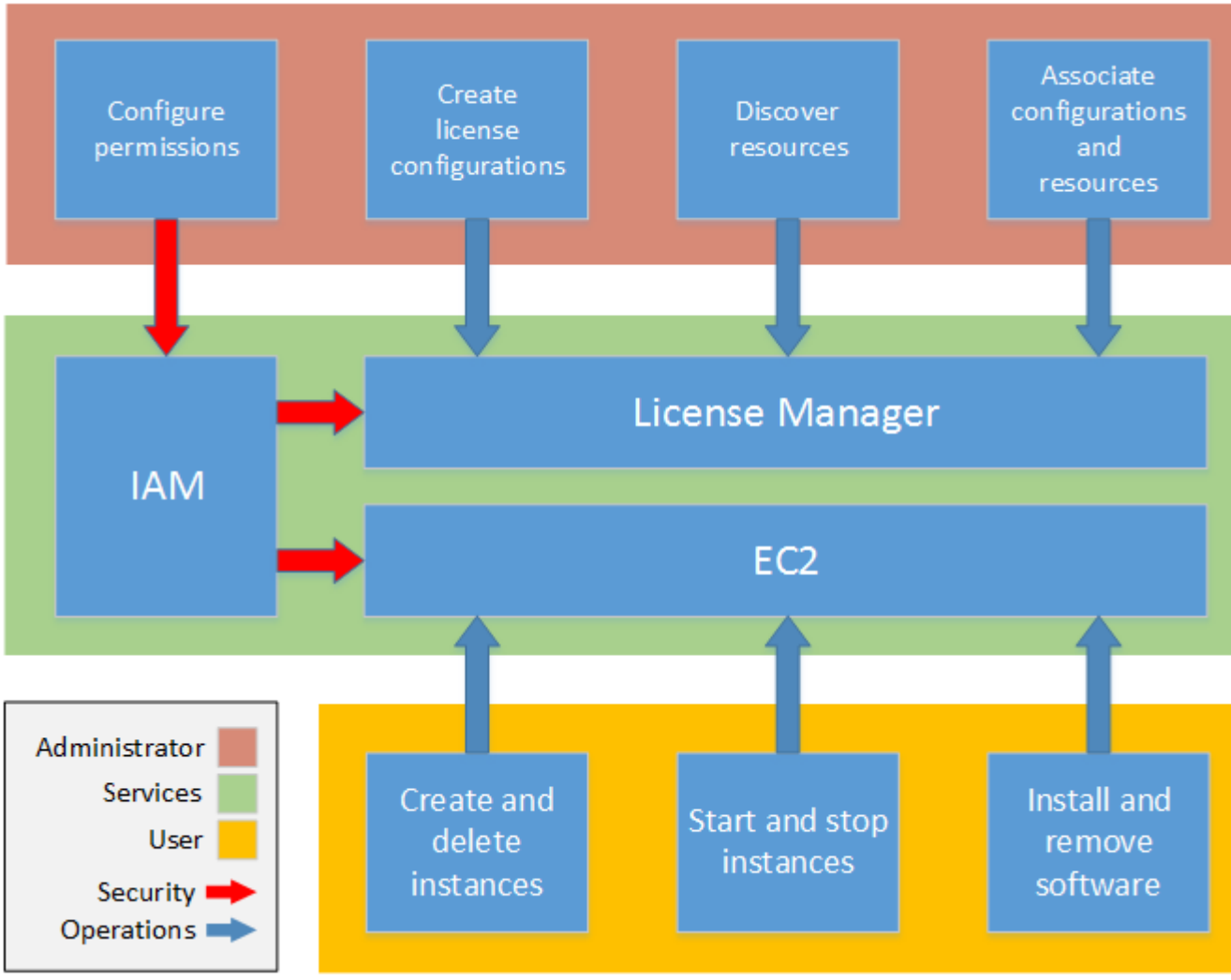
How License Manager works

Effective software license management relies on the following:

- An expert understanding of language in enterprise licensing agreements
- Appropriately restricted access to operations that consume licenses
- Accurate tracking of license inventory

Enterprises are likely to have dedicated persons or teams responsible for each of these domains. It then becomes a problem of effective communication, particularly between license experts and system administrators. License Manager provides a way of pooling knowledge from various domains. Crucially, it also integrates natively with AWS services—for example, with the Amazon EC2 control plane where instances are created and deleted. This means that License Manager rules and limits capture business and operational knowledge, and also translate to automated controls on instance creation and application deployment.

The following diagram illustrates the distinct but coordinated duties of license administrators, who manage permissions and configure License Manager, and users, who create, manage, and delete resources through the Amazon EC2 console.



If you are responsible for managing licenses in your organization, you can use License Manager to set up licensing rules, attach them to your launches, and keep track of usage. The users in your organization can then add and remove license-consuming resources without additional work.

A licensing expert manages licenses across the entire organization, determining resource inventory needs, supervising license procurement, and driving compliant license usage. In an enterprise using License Manager, this work is consolidated through the License Manager console. As shown in the diagram, this involves setting service permissions, creating rule-based license configurations, taking inventory of computing resources both on-premises and in the cloud, and associating license configurations with discovered resources. In practice, this could mean associating a license configuration with an approved Amazon Machine Image (AMI) that IT uses as a template for all Amazon EC2 instance deployments.

License Manager saves costs that would otherwise be lost to license violations. While internal audits reveal violations only after the fact, when it is too late to avoid penalties for non-compliance, License Manager prevents expensive incidents from ever occurring. License Manager simplifies reporting with built-in dashboards showing license consumption and resources tracked.

Getting started with AWS License Manager

To begin using AWS License Manager, log into the License Manager console.

To get started with License Manager

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/. You are prompted to configure permissions for License Manager and its supporting services. Follow the directions.
2. Create a license configuration and attach it to your AMIs and instances.
3. Launch instances and track license usage using the built-in dashboards.

Working with AWS License Manager

License Manager can be applied to standard scenarios for enterprises with a mixed infrastructure of AWS resources and on-premises resources. You can create license configurations, take inventory of your license-consuming resources, associate licenses with resources, and track inventory and compliance.

Licensing for AWS Marketplace products

Using License Manager, you can now associate licensing rules to AWS Marketplace BYOL AMI products via Amazon EC2 launch templates, AWS CloudFormation templates, or AWS Service Catalog products. In each case, you benefit from centralized license-tracking and compliance enforcement.

> **Note**
> License Manager does not change how you obtain and activate your BYOL AMIs from Marketplace. After launching, you must provide a license key obtained directly from the seller to activate any third-party software.

Tracking licenses for resources in on-premises data centers

With License Manager, you can discover applications running outside of AWS with the Systems Manager inventory, and then attach licensing rules to them. After licensing rules are attached, you can track on-premises servers along with AWS resources in the License Manager console.

Differentiate between license included and BYOL

With License Manager, you can identify which resources have a license that is included with the product and which use a license that you own. This enables you to accurately report how you are using BYOL licenses. This filter requires SSM version 2.3.722.0 or later.

License Manager across your AWS accounts

License Manager enables you to manage licenses across your AWS accounts. You can create license configurations once in your AWS Organizations management account and share them across your accounts using AWS Resource Access Manager or by linking AWS Organizations accounts using License Manager settings. This also enables you to perform cross-account discovery to search inventory across your AWS accounts. However, the following Regions do not support license management across AWS accounts:

- China (Beijing)
- China (Ningxia)

Contents

License configurations in License Manager

License configurations are the core of License Manager. They contain licensing rules based on the terms of your enterprise agreements. The rules that you create determine how AWS processes commands that consume licenses. While creating license configurations, work closely with your organization's compliance team to review your enterprise agreements.

Limits

- Number of license configurations per resource: 10
- Total number of license configurations: 25
- Systems Manager managed instances must be associated with vCPU and instance type license configurations.

Contents

License configuration parameters and rules

A license configuration consists of basic parameters and rules that vary according to the parameter values. You can also add tags to your license configurations. After you create a license configuration, an administrator can modify the number of licenses and the usage limit to reflect changing resource needs.

Available parameters and rules include the following:

- **Name** — The name of the license configuration.
- **Description** — A description of the license configuration.
- **License counting type** — The metric used to count licenses. Supported values are physical core, vCPU, socket, and instance.
- **(Optional) License count** — The number of licenses managed by this configuration.
- **(Optional) License count hard limit** — The kind of limit represented by the license count. A hard limit blocks the launch of an out-of-compliance instance. A soft limit permits out-of-compliance launches but sends an alert when one occurs.
- **Number of licenses consumed** - The number of licenses used by a resource.
- **Status** — Indicates whether the configuration is active.
- **Product information** — The names and versions of the products for automated discovery (p. 27). The supported products are Windows Server, SQL Server, and Oracle Database.
- **(Optional) Rules** - These include the following. Available rules vary by counting type.
  - **License affinity to host (in days)** — Restricts license usage to the host for the specified number of days. The range is 1 to 180. The counting type must be Cores or Sockets. After the affinity period elapses, the license will be available for reuse within 24 hours.
  - **Maximum cores** — Maximum count cores for a resource.
  - **Maximum sockets** — Maximum count sockets for a resource.

- **Maximum vCPUs** — Maximum count vCPUs for a resource.
- **Minimum cores** — Minimum count cores for a resource.
- **Minimum sockets** — Minimum count sockets for a resource.
- **Minimum vCPUs** — Minimum count vCPUs for a resource.
- **Tenancy** — Restricts license usage to the specified EC2 tenancy. Dedicated Hosts are required if the counting type is Cores or Sockets. Shared tenancy, Dedicated Hosts, and Dedicated Instances are supported if the counting type is Instances or vCPUs. The console (and API) names are as follows:
  - **Shared** (`EC2-Default`)
  - **Dedicated Instance** (`EC2-DedicatedInstance`)
  - **Dedicated Host** (`EC2-DedicatedHost`)
- **vCPU Optimization** — License Manager integrates with CPU optimization support in Amazon EC2, which enables you to customize the number of vCPUs on an instance. If this rule is set to True, License Manager counts vCPUs based on the customized core and thread count. Otherwise, License Manager counts the default number of vCPUs for the instance type.

The following table describes which license rules are available for each counting type.

Console name	API name	Cores	Instances	Sockets	vCPUs
License affinity to host (in days)	`licenseAffinityToHost`	♦		♦	
Maximum cores	`maximumCores`	♦	♦		
Maximum sockets	`maximumSockets`		♦	♦	
Maximum vCPUs	`maximumVcpus`		♦		♦
Minimum cores	`minimumCores`	♦	♦		
Minimum sockets	`minimumSockets`		♦	♦	
Minimum vCPUs	`minimumVcpus`		♦		♦
Tenancy	`allowedTenancy`	♦	♦	♦	♦
vCPU Optimization	`honorVcpuOptimization`				♦

Build License Manager rules from vendor licenses

You can create License Manager rule sets based on the language of software vendor licenses. The examples that follow are not intended as blueprints for actual use cases. In any real-world application of a license agreement, you choose among competing options depending on the architecture and licensing history of your particular on-premises server environment. Your options also depend on the details of your planned migration of resources to AWS.

As much as possible, these examples are meant to be vendor-neutral, focusing instead on generally applicable questions of hardware and software allocation. Vendor licensing provisions interact as well with AWS requirements and limits. The number of licenses required for an application varies according to the instance type chosen and other factors.

Important
AWS does not participate in the audit process with software vendors. Customers are responsible for compliance and assume the responsibility of carefully understanding and capturing rules into License Manager based on their licensing agreements.

Example: Implementing an operating system license

This example involves a license for a server operating system. The licensing language imposes constraints on the type of CPU core, tenancy, and minimum number of licenses per server.

In this example, the licensing terms include the following stipulations:

- Physical processor cores determine the license count.
- The number of licenses must equal the number of cores.
- A server must run a minimum of eight cores.
- The operating system must run on a non-virtualized host.

In addition, the customer has made the following decisions:

- Licenses for 96 cores have been purchased.
- A hard limit is imposed to restrict license consumption to the quantity purchased.
- Each server needs a maximum of 16 cores.

The following table associates the License Manager rule-making parameters with the vendor licensing requirements that they capture and automate. The example values are for illustration purposes only; you would specify the values that you need in your own license configurations.

License Manager Rule	Settings
License counting type	**License Type** is set to **`Cores`**.
License count	**Number of cores** is set to **`96`**.
Minimum / Maximum vCPUs or cores	**Minimum cores** is set to **`8`**. **Maximum cores** is set to **`16`**.
License count hard limit	**Enforce license limit** is selected.
Allowed tenancy	**Tenancy** is set to **`Dedicated Host`**.

Create a license configuration

A license configuration represents the licensing terms in the agreement with your software vendor. Your license configuration specifies how your licenses should be counted (for example, by vCPUs or number of instances). It also specifies limits on your usage, so that you can prevent usage from going over the number of allocated licenses. Additionally, it can also specify other constraints on your licenses, such as the tenancy type.

Requirements for Oracle Database products

When you add product information to configure automated discovery of Oracle Database products, the following requirements apply:

- The supported license counting type is `vCPU`.
- Rules are not supported.
- Hard license limits are not supported.
- You can track one product version per license configuration.
- You cannot track Oracle products and other products using the same license configuration.

To create a license configuration using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Choose **Create license configuration**.
4. In the **Configuration details** panel, provide the following information:
   - **License configuration name** — A name for the license configuration.
   - **Description** — An optional description of the license configuration.
   - **License type** — The counting model for this license (**vCPUs**, **Cores**, **Sockets**, or **Instances**).
   - **Number of <option>** — The option displayed depends on the license type. When the license limit is exceeded, License Manager notifies you (soft limit) or prevents a resource from deploying (hard limit).
   - **Enforce license limit** — If selected, the license limit is a hard limit.
   - **Rules** — One or more rules. For each rule, select a rule type, provide a rule value, and choose **Add rule**. The rule types displayed depend on the license type. For example, minimum values, maximum values, and tenancy. If you do not specify a tenancy type, all are accepted.
5. (Optional) In the **Automated discovery rules** panel, do the following:
   a. Choose the product name, product type, and resource type for each product to discover and track using automated discovery (p. 27).
   b. Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
   c. (Optional) If your account is a License Manager management account for an Organizations you have to option to define resources to exclude from automated discovery. To do so select **Add exclusion rule**, choose the property to filter on, AWS account IDs and resource Tags are supported, then enter the information to identify that property.
6. (Optional) Expand the **Tags** panel to add one or more tags to your license configuration. Tags are key/value pairs. Provide the following information for each tag:
   - **Key** — The searchable name of the key.
   - **Value** — The value for the key.
7. Choose **Submit**.

To create a license configuration using the command line

- create-license-configuration (AWS CLI)
- New-LICMLicenseConfiguration (Tools for Windows PowerShell)

Share a license configuration

You can use AWS Resource Access Manager to share your license configurations with any AWS account or through AWS Organizations. For more information, see the AWS RAM User Guide.

Edit a license configuration

You can edit values for the following fields in a license configuration:

- Name
- Description

- License count
- License count hard limit

To edit a license configuration

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Select the license configuration.
4. Choose **Actions**, **Edit**.
5. Edit the details as needed and then choose **Update**.

To edit a license configuration using the command line

- update-license-configuration (AWS CLI)
- Update-LICMLicenseConfiguration (Tools for Windows PowerShell)

Deactivate a license configuration

When you deactivate a license configuration, existing resources using the license are unaffected and AMIs using the license can still be launched. However, license consumption is no longer tracked.

When a license configuration is deactivated, it must not be attached to any running instance. After deactivation, launches cannot be performed with the license configuration.

To deactivate a license configuration

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Select the license configuration.
4. Choose **Actions**, **Deactivate**. When prompted for confirmation, choose **Deactivate**.

To deactivate a license configuration using the command line

- update-license-configuration (AWS CLI)
- Update-LICMLicenseConfiguration (Tools for Windows PowerShell)

Delete a license configuration

Before you can delete a license configuration, you must disassociate any resources. You can delete a license configuration if you need to start over with new licensing rules. If the licensing terms from your software vendors change, you can disassociate existing resources, delete the license configuration, create a new license configuration to reflect the updated terms and associate it with the existing resources.

To delete a license configuration using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Choose the name of the license configuration to open the license details page.
4. Select each resource (individually or in bulk) and choose **Disassociate resource**. Repeat until the list is empty.

5. Choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.

To delete a license configuration using the command line

- delete-license-configuration (AWS CLI)
- Remove-LICMLicenseConfiguration (Tools for Windows PowerShell)

License rules in License Manager

After license configuration rules are in place, they can be attached to the relevant launch mechanisms, where they can directly prevent the deployment of new resources that are non-compliant. Users in your organization can seamlessly launch EC2 instances from designated AMIs, and administrators can track license inventory through the built-in License Manager dashboard. Launch controls and dashboard alerts allow easier compliance enforcement.

> **Important**
> AWS does not participate in the audit process with software vendors. Customers are responsible for compliance and assume the responsibility of carefully understanding and capturing rules into License Manager based on their licensing agreements.

License tracking works from the time rules are attached to an instance until its termination. You define your usage limits and licensing rules, and License Manager tracks deployments while also alerting you to rule violations. If you have configured hard limits, License Manager can prevent resources from launching.

When a tracked server is stopped or terminated, its license is released and returned to the pool of available licenses.

Because organizations have differing approaches to operations and compliance, License Manager supports multiple launch mechanisms:

- **Manual association of license configurations with AMIs** — For tracking licenses for operating system or other software, you can attach licensing rules to AMIs before publishing them for broader use in your organization. Any deployments from these AMIs are then automatically tracked with License Manager without requiring any additional actions by users. You can also attach licensing rules to your current AMI building mechanisms such as Systems Manager Automation, VM Import/Export, and Packer.
- **Amazon EC2 launch templates and AWS CloudFormation** — If attaching licensing rules to AMIs is not a preferred option, you can specify them as optional parameters in EC2 launch templates or AWS CloudFormation templates. Deployments using these templates are tracked using License Manager. You can enforce rules on EC2 launch templates or AWS CloudFormation templates by specifying one or more license configuration IDs in the **License Configurations** field.

AWS treats license-tracking data as sensitive customer data accessible only through the AWS account that owns it. AWS does not have access to your license-tracking data. You control your license-tracking data and you can delete it at any time.

Associating license configurations and AMIs

The following procedure demonstrates how to associate license configurations with AMIs using the License Manager console. The procedure assumes that you have at least one existing license configuration. You can associate license configurations with any AMI that you have access to, whether owned or shared. If an AMI was shared with you, you can associate it with the license configuration in the current account. Otherwise, you can specify whether the AMI is associated with the license configuration across all accounts or only in the current account.

If you associate an AMI with a license configuration across all accounts, you can track instance launches from the AMI across accounts. When a hard limit is reached, License Manager blocks additional instance launches. When a soft limit is reached, License Manager notifies you of additional instance launches. You must ensure that users can't get access to the AMI through another mechanism, such as copying the AMI or creating an AMI from an instance launched from the AMI.

To associate a license configuration and an AMI

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Choose the name of the license configuration to open the license details page. To view the currently associated AMIs, choose **Associated AMIs**.
4. Choose **Associate AMI**.
5. For **Available AMIs**, select one or more AMIs and choose **Associate**.
   - If your account owns at least one of the AMIs, you are prompted to choose an AMI association scope for the AMIs that you own. Any AMIs that were shared with from another account are associated with only your account. Choose **Confirm**.
   - If the AMIs were shared with you from another account, they are associated with only your account.

   The newly associated AMIs now appear on the **Associated AMIs** tab on the license details page.

Disassociating license configurations and AMIs

The following procedure demonstrates how to disassociate license configurations from AMIs using the License Manager console. You cannot disassociate a deregistered AMI. License Manager checks for deregistered AMIs every 8 hours and automatically disassociates them.

To disassociate a license configuration and an AMI

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configurations**.
3. Choose the name of the license configuration to open the license details page.
4. Choose **Associated AMIs**.
5. Select the AMI and choose **Disassociate AMI**.

License reporting in License Manager

Using AWS License Manager you can track the history of your license configurations by scheduling periodic snap shots of your license usage. By setting up report generators License Manager will automatically upload reports of your license configurations to an S3 bucket based on your specifications. You can set up multiple report generators to effectively track configurations of different license types in your environment.

Note
AWS License Manager does not store your reports. License Manager reports are published directly to your S3 bucket. Once you delete a report generator, reports are no longer published to your S3 bucket.

Creating a report generator

When you create a report generator you specify a license configuration type for License Manager to track, a frequency interval that defines how often to generate reports, and a report type. All reports are

generated in CSV format and published to an S3 bucket. A report generator can produce one or more of following report types.

License configuration report

This report type contains information on the number of consumed licenses and details about license configuration. The tracked license configuration type is listed with details such as the license count, license rules, and the distribution of licenses across different resource types.

Resource report

This report type gives you details about your tracked resources and their license consumption. Each tracked resource using the specified license configuration type is listed with details such as the license ID, the status of the resource, and the AWS account ID that owns the resource.

To create a report generator

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. From the navigation panel choose **Reports**. Then, from the **Create report generator** pane define the parameters for the report:
   a. Enter a **Name** and optional **Description** for your generator.
   b. Select a license configuration type from the drop down list. This is the type of license that the report generator will be generating data on.
   c. Choose the report types to generate.
   d. Choose the frequency by which License Manager will publish the reports, you can choose **Once every day**, **Once every week** or **Once every month**.
   e. (Optional) Add **Tags** to track the report generator resource.
3. Select **Create report generator**.

A new report generator will begin publishing reports within 60 minutes or less.

If you do not already have an S3 bucket associated with your account, License Manager will create a new Amazon S3 bucket in your account when you create a report generator. If you have previously enabled **Cross-account inventory search** reports will be sent to the S3 bucket created by License Manager when **Cross-account inventory search** was enabled.

Reports are stored in your bucket with the following Amazon S3URI pattern:

```
s3://aws-license-manager-service-*/Reports/report-generator-name/year/months/day/report-id.csv
```

Editing your report generators

You can view and make changes to your report generators from the License Manager console at any time. The **Report generators** table lists all the report generators created for your account, from the table you can get an overview of your different reports, pivot to the Amazon S3 bucket associated with your report generators, and view the status of report generation.

To edit a report generator

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. From the navigation panel choose **Reports**.
3. Choose the report generator you want to edit from the table, then select **View details**.
4. Select **Edit** to make changes to the report generator.

5. Make the desired changes to your report generator then choose **Save changes**.

An updated report generator will generate a new report within an hour.

> **Note**
> Changing the name of your report generator will send future reports to a new folder in your License Manager S3 bucket reflecting the new name.

Deleting a report generator

Deleting a report generator stops the generation of new reports, however, your Amazon S3 bucket and all your previous reports are not affected.

> **Note**
> You will be unable to delete a license configuration from your account if it has a report generator associated with. You must first delete that report generator.

To edit a report generator

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. From the navigation panel choose **Reports**.
3. Choose the report generator you want to edit from the table, then select **View details**.
4. Select **Delete**. This action permanently deletes the report generator.

License type conversions in License Manager

You can change your license type between AWS provided licensing and Bring Your Own License (BYOL) as your business needs change, without redeploying your existing workloads.

You can optimize your license inventory for the following scenarios using license type conversion:

Migrate on-premises workloads to Amazon EC2

During your migration, you can deploy your workload to Amazon EC2 and use AWS provided licenses. When the migration is complete, use License Manager license type conversion to change the license type of your instances to BYOL so that you can use the licenses that were released during the migration.

Continue running workloads with expiring license agreements

If your license agreement with Microsoft is about to expire and you do not plan to renew it, you can use License Manager license type conversion to switch from BYOL to AWS provided licenses. This switch allows you to continue running your workloads with fully compliant software licenses provided by AWS with a flexible pay-as-you go licensing model.

Optimize costs

For small or irregular workloads, license-included instances might be more cost effective than running BYOL because BYOL might require a longer term commitment. For this case, you can use License Manager license type conversion to switch your instances to use AWS provided licenses to optimize licensing related costs. Additionally, when your workload is more steady or predictable, you can easily switch back to BYOL and use licensed media acquired directly from your software vendor if your instances were launched from your own virtual machine (VM) image.

License type conversion topics

- Eligible license types for license type conversion (p. 16)

Eligible license types for license type conversion

License type conversion is available for Windows Server and SQL Server licenses.

Supported SQL Server editions:

- SQL Server Standard edition
- SQL Server Enterprise edition
- SQL Server Web edition

A conversion task changes the usage operation value associated with your instance. Usage operation values for each supported platform are provided in the following table. For more information, see AMI billing information fields.

Platform details	Usage operation
Windows Server License Included	RunInstances:0002
Windows Server BYOL	RunInstances:0800
Windows Server License Included with SQL Server Standard License Included	RunInstances:0006
Windows Server License Included with SQL Server Enterprise License Included	RunInstances:0102
Windows Server License Included with SQL Server Web License Included	RunInstances:0202
Windows Server License Included with SQL Server (any edition) BYOL	RunInstances:0002
Windows Server BYOL with SQL Server (any edition) BYOL	RunInstances:0800

Prerequisites

To convert license types with License Manager, verify that the following prerequisites are met:

- Your AWS account must be onboarded to License Manager. See Getting started with AWS License Manager (p. 5).
- The target instance must be in a stopped state before you convert the license type. When a license conversion task is in progress, you can start and stop the target instance.
- The target instance must be configured with AWS Systems Manager Inventory and include the following permissions:
  - `ssm:GetInventory`
  - `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `license-manager:CreateLicenseConversionTaskForResource`
- `license-manager:GetLicenseConversionTask`
- `license-manager:ListLicenseConversionTasks`
- `license-manager:GetLicenseConfiguration`
- `license-manager:ListUsageForLicenseConfiguration`
- `license-manager:ListLicenseSpecificationsForResource`
- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`

  For more information about Systems Manager Inventory, see AWS Systems Manager Inventory.
- The original Amazon EC2 instance must be launched from your own virtual machine (VM) image. For more information about converting a VM to Amazon EC2, see VM Import/Export. Instances that were originally launched from an Amazon Machine Image (AMI) are not eligible for license type conversion to BYOL.

Convert a license type

You can convert license types using the AWS CLI. When you create a license type conversion task, License Manager validates the billing products on your instance. If these preliminary validations are successful, License Manager creates a license type conversion task. You can check the status of a license conversion task by using the `list-license-conversion-tasks` and `get-license-conversion-task` AWS CLI commands.

License Manager might update the resources associated with your customer managed licenses as part of a conversion task. Specifically, for any customer managed license with automated discovery rules of type `License Included`, License Manager disassociates the resource in the license type conversion task from the license if the `License Included` automated discovery rule explicitly excludes the resource.

For example, if your customer managed license contains two automated discovery rules, and each rule excludes license included Windows Server, then a license type conversion from BYOL to license included Windows Server results in disassociation of the instance from the customer managed license. However, if only one of the two automated discovery rules contains a `License Included` rule, then the instance is not disassociated.

When the license type conversion task succeeds, its status changes from `IN_PROGRESS` to `SUCCEEDED`. If License Manager encounters issues during the workflow, it updates the status of the license type conversion task to `FAILED`, and updates the status message with an error message.

> **Note**
> The billing product information on the AMI used to launch an instance does not change when you convert the license type. To retrieve accurate billing information, use the Amazon EC2 `DescribeInstances` API. Additionally, if you have existing workflows that search for billing information from AMIs, update those workflows to use `DescribeInstances`.

License type conversion topics

- License type conversion limits (p. 18)

License type conversion limits

Important
The use of Microsoft software is subject to the licensing terms of Microsoft. You are responsible for complying with Microsoft licensing terms. This documentation is provided for convenience, and you are not entitled to rely on its description. This documentation does not constitute legal advice. If you have questions about your licensing rights to Microsoft software, consult with your legal team, Microsoft, or your Microsoft reseller.

License Manager restricts the types of license conversion tasks that you can create in accordance with the Microsoft Service Provider License Agreement (SPLA). Some of the restrictions that license type conversion is subject to are listed as follows. This is not a comprehensive list and is subject to change.

- The Amazon EC2 instance must be launched from your own virtual machine (VM) image.
- License included SQL Server cannot be run on a Dedicated Host.
- A license included SQL Server instance must have at least 4 vCPUs.

Convert a license type using the AWS CLI

To start a license type conversion task in the AWS CLI:

Determine the license type of your instance

1. Verify that you have installed and set up the AWS CLI. For more information, see Installing, updating, and uninstalling the AWS CLI and Configuring the AWS CLI.
2. Verify that you have permissions to run the `create-license-conversion-task-for-resource` AWS CLI command. For help with this, see Example policies for License Manager (p. 43).
3. To determine the license type currently associated with your instance, run the following AWS CLI command. Replace the instance ID with the ID of the instance for which you want to determine the license type.

```
aws ec2 describe-instances -instance-id <instance-id>
```

4. The following is an example response to the `describe-instances` command. Note that the `UsageOperation` value is the billing information code associated with the license. The `UsageOperationUpdateTime` is the time when the billing code was updated. For more information, see DescribeInstances in the *Amazon EC2 API reference*.

```
"InstanceId": "<instance-id>",
"Platform details": "Windows with SQL Server Enterprise",
"UsageOperation": "RunInstances:0800",
"UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
```

Note
The usage operation for Windows Server with SQL Enterprise BYOL is the same as the usage operation for Windows BYOL because they are identically billed.

Convert Windows Server from license included to BYOL

When you convert Windows Server from license included to BYOL, License Manager does not automatically activate Windows. You must switch the KMS server for your instance from the AWS KMS server to your own KMS server.

Important
In order to convert from license included to BYOL, the original Amazon EC2 instance must be launched from your own virtual machine (VM) image. For more information about converting a VM to Amazon EC2, see VM Import/Export. Instances that were originally launched from an Amazon Machine Image (AMI) are not eligible for license conversion to BYOL.

Check your Microsoft license agreement to determine what methods you can use to activate Microsoft Windows Server. For example, if you are using a KMS server, you must obtain the address of your KMS server from the original BYOL configuration of the instance.

1. To convert the license type of your instance, run the following command, replacing the ARN with the ARN of the instance you want to convert.

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0002 \
    --destination-license-context UsageOperation=RunInstances:0800
```

2. To activate Windows after you convert your license, you must point the Windows Server KMS server for your operating system to your own KMS servers. Log in to the Windows instance and run the following command.

```
slmgr.vbs /skms <your-kms-address>
```

Convert Windows Server from BYOL to license included

When you convert Windows Server from BYOL to license included, License Manager automatically switches the KMS server for your instance to the AWS KMS server.

To convert the license type of your instance from BYOL to license included, run the following command, replacing the ARN with the ARN of the instance you want to convert.

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0800 \
    --destination-license-context UsageOperation=RunInstances:0002
```

Convert Windows Server from license included to BYOL and SQL Server Standard from BYOL to license included

You can switch multiple products at the same time, and in multiple directions. For example, you can convert both Windows Server and SQL Server in one license type conversion task.

To convert the license type of your Windows Server instance from license included to BYOL, and SQL Server Standard from BYOL to license included, run the following command, replacing the ARN with the ARN of the instance you want to convert.

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0002 \
    --destination-license-context UsageOperation=RunInstances:0804
```

Tenancy conversion

You can change the tenancy of your instance to best suit your use case. You can use the modify-instance-placement AWS CLI command to switch among the following tenancies:

- Shared
- Dedicated Instance
- Dedicated Host
- Host Resource Groups (HRG)

Your account must have a Dedicated Host with available capacity to start the instance in order to switch to the Dedicated Host tenancy type. To move to the Host Resource Groups tenancy type, you must have at least one HRG in your account.

Tenancy conversion limits

The following limits apply to tenancy conversion:

- The Linux billing code is permitted on all tenancy types.
- The Windows BYOL billing code is not permitted on Shared tenancy.
- The Windows Server license included billing code is permitted on all tenancy types.
- All supported SQL Server editions, Red Hat (RHEL), and SUSE (SLES) license included billing codes are permitted on Shared tenancy and Dedicated Instances. However, these billing codes are not permitted on Dedicated Hosts and Host Resource Groups.
- License included billing codes other than Windows Server are not permitted on Dedicated Hosts and Host Resource Groups.

Change the tenancy of an instance using the AWS CLI

An instance must be in the `stopped` state in order to change its tenancy.

To stop the instance, run the following command.

```
aws ec2 stop-instances --instance-ids <instance_id>
```

To change an instance from any tenancy to `default` or `dedicated` tenancy, run the following commands.

`default`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy default
```

`dedicated`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy dedicated
```

To change an instance from any tenancy to `host` tenancy with auto-placement, run the following command.

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --affinity default
```

To change an instance from any tenancy to `host` tenancy, targeting a specific Dedicated Host, run the following command.

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
```

```
  --tenancy host --affinity host --host-id <host_id>
```

To change an instance from any tenancy to `host` tenancy using a Host Resource Group, run the following command.

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --host-resource-group-arn <host_resource_group_arn>
```

Troubleshooting license type conversion

Incomplete license type conversion tasks

License type conversion tasks contain multiple steps. In some cases, when you convert Windows Server instances from BYOL to license included, the billing products on an instance are successfully updated. However, the KMS server might not switch to the AWS KMS server.

To remediate this issue, follow the steps in Why did Windows activation fail on my EC2 Windows instance? to activate Windows either with the Systems Manager AWSSupport-ActivateWindowsWithAmazonLicense Automation runbook, or log in to the instance and manually make the switch to the AWS KMS server.

Host resource groups in AWS License Manager

A Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. A host resource group is a collection of Dedicated Hosts that you can manage as a single entity. As you launch instances, License Manager allocates the hosts and launches instances on them based on the settings that you configured. You can add existing Dedicated Hosts to a host resource group and take advantage of automated host management through License Manager.

You can use host resource groups to separate hosts by purpose, for example, development test hosts versus production, organizational unit, or license constraint. After you add a Dedicated Host to a host resource group, you cannot launch instances directly on the Dedicated Host, you must launch them using the host resource group.

Settings

You can configure the following settings for a host resource group:

- **Allocate hosts automatically**–Indicates whether Amazon EC2 can allocate new hosts on your behalf if launching an instance in this host resource group would exceed its available capacity.
- **Release hosts automatically**–Indicates whether Amazon EC2 can release unused hosts on your behalf. An unused host has no running instances.
- **Recover hosts automatically**–Indicates whether Amazon EC2 can move instances from a host that has failed unexpectedly to a new host.
- **Associated license configurations**–The license configurations that can be used to launch instances in this host resource group.
- **Instance families**–The types of instances that you can launch. By default, you can launch any instance types that are supported on a Dedicated Host. If you launch Nitro-based instances, then you can launch instances with different instance types in the same host resource group. Otherwise, you must launch only instances with the same instance type in the same host resource group.

Contents

Create a host resource group

Configure a host resource group to enable License Manager to manage your Dedicated Hosts. To best utilize your most expensive licenses, you can associate one or more core- or socket-based license configurations with your host resource group. To best optimize host utilization, you can allow all core- or socket-based license configurations with your host resource group.

To create a host resource group

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Choose **Create host resource group**.
4. For **Host resource group details**, specify a name and description for the host resource group.
5. For **EC2 Dedicated Host management settings**, enable or disable the following settings as needed:
   - **Allocate hosts automatically**
   - **Release hosts automatically**
   - **Recover hosts automatically**
6. (Optional) For **Additional settings**, select the instance families that you can launch in the host resource group.
7. For **License configurations**, select one or more core- or socket-based license configurations.
8. (Optional) For **Tags**, add one or more tags.
9. Choose **Create**.

Share a host resource group

You can use AWS Resource Access Manager to shared your host resource groups through AWS Organizations. After you share a host resource group and license configuration, member accounts can launch instances into the shared host resource group. The new hosts are allocated in the account that owns the host resource group. The member account owns the instances. For more information, see the AWS RAM User Guide.

Launch an instance in a host resource group

When you launch an instance, you can specify a host resource group. For example, you can use the following run-instances command. You must associate a core- or socket-based license configuration with the AMI.

```
aws ec2 run-instances --min-count 2 --max-count 2 \
--instance-type c5.2xlarge --image-id ami-0abcdef1234567890 \
--placement="Tenancy=host,HostResourceGroupArn=arn"
```

You can also use the Amazon EC2 console. For more information, see Launching Instances into a Host Resource Group in the *Amazon EC2 User Guide*.

Modify a host resource group

You can modify the settings for a host resource group at any time. You cannot set the host limit lower than the number of existing hosts in the host resource group. You cannot remove an instance type if there's an instance of that type running in the host resource group.

To modify a host resource group

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Select the host resource group and choose **Actions**, **Edit**.
4. Modify the settings as needed.
5. Choose **Save changes**.

Delete a host resource group

You can delete a host resource group if it has no hosts.

To delete a host resource group

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Select the host resource group and choose **Actions**, **Delete**.
4. When prompted for confirmation, choose **Delete**.

Adding Dedicated Hosts to a host resource group

You can add your existing hosts to a host resource group from the AWS Management Console, AWS CLI, or AWS API. To add your hosts, you must be the AWS account owner where you created the Dedicated Host and host resource groups. If your host resource group lists allowed license configurations and instances types, the host you add must match these requirements.

> **Note**
> Suppose you stop the instances and want to restart them. You must perform the following two tasks:
>
> - Modify the instance to point to the host resource group.
> - Associate license configurations to match the host resource group.

For more information about Resource Groups, see AWS Resource Groups User Guide.

Use the following steps to add one or more Dedicated Hosts to a resource group:

1. Log into the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Host Resource Groups**.
3. From the list of host resource group names, click on the name of the host resource group where you want to add the Dedicated Host.
4. Choose **Dedicated Hosts**.

5. Choose **Add**.
6. Choose one or more Dedicated Hosts to add to the host resource group.
7. Choose **Add**.

   Adding the host may take 1 - 2 minutes, and then it appears in the list of **Dedicated Hosts.**

Removing Dedicated Hosts from a host resource group

When you remove a host from the host resource group, the instance running on the host remains on the host. The instances attached to the host resource group remain associated with the group, and instances directly attached to the host through affinity maintain the same property. If you share the host resource group with other AWS accounts, License Manager automatically removes the shared host and consumers receive an eviction notice to move their instances from the host in 15 days.

Use the following steps to remove a Dedicated Host to a host resource group:

1. Log into the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Host Resource Groups**.
3. Click on the name of the host resource that you want to remove a Dedicated Host.
4. Choose **Dedicated Hosts**.
5. Choose the Dedicated Host to delete from the host resource group. Or, you can search for a Dedicated Host by host ID, host type, host state, or availability zone.
6. Choose **Remove**.
7. Choose **Remove** again to confirm.

Resource inventory in License Manager

License Manager allows you to discover on-premises applications using Systems Manager inventory, and then to attach licensing rules to them. After licensing rules are attached to these servers, you can track them along with your AWS servers in the License Manager dashboard.

License Manager cannot, however, validate licensing rules for these servers at launch or termination time. To keep information about non-AWS servers up-to-date, you must periodically refresh the inventory information using the **Search inventory** section of the License Manager console.

Systems Manager stores data in its Inventory data for 30 days. During this period, License Manager counts a managed instance as active even if it is not pingable. After inventory data has been purged from Systems Manager, License Manager marks the instance as inactive and updates local inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in Systems Manager so that License Manager can run cleanup operations.

Querying Systems Manager inventory requires a Resource Data Sync to store inventory in an Amazon S3 bucket, Amazon Athena to aggregate inventory data from organizational accounts, and AWS Glue to provide a fast query experience. For more information, see Using service-linked roles for AWS License Manager (p. 44).

Resource inventory tracking is also useful if your organization does not restrict AWS users from creating AMI-derived instances or installing additional software on running instances. License Manager provides you with a mechanism to easily discover these instances and applications using inventory search. You can attach rules to these discovered resources and track and validate them the same as instances created from managed AMIs.

Contents

Discover resource inventory

License Manager uses Systems Manager inventory to discover software usage on premises. After you associate a license configuration with on-premises servers, License Manager periodically collects software inventory, updates licensing information, and refreshes its dashboards to report usage.

Tasks

Setting up for inventory search

Complete the following requirements before using resource inventory search:

- Enable cross-account inventory discovery by integrating License Manager with your AWS Organizations account. For more information, see Settings in License Manager (p. 39).
- Create license configurations for the servers and applications to manage. For example, create a license configuration that reflects the terms of your licensing agreement with Microsoft for SQL Server Enterprise.

Using inventory search

Complete the following steps to search your resource inventory. You can search for applications by name (for example, names that begin with "SQL Server") and the type of license included (for example, a license that is not for "SQL Server Web").

To search your resource inventory

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Search inventory**.
3. Specify filter options to scope the list of displayed resources.

   The following filters and logical operators are supported for Amazon EC2 resources:

   - **Resource ID** – The ID of the resource. Logical operators are **Equals** and **Not equals**.
   - **Account ID** – The ID of the AWS account that owns the resource. Logical operators are **Equals** and **Not equals**.
   - **Platform name** – The platform of the resource. Logical operators are **Equals**, **Not equals**, **Begins with**, and **Contains**.
   - **Application name** – The name of the application. Logical operators are **Equals** and **Begins with**.
   - **License included name** – The type of license included. Logical operators are **Equals** and **Not equals**. Possible values are **SQL Server Enterprise**, **SQL Server Standard**, **SQL Server Web**, and **Windows Server Datacenter**.

- **Tag** – The key/value combination of a tag assigned to the resource. The tag value is optional. Logical operators are **Equals** and **Not equals**. **Not equals** is shown only if cross account discovery is enabled.

The following filters and logical operators are supported for Amazon RDS resources:

- **Engine Edition**– The edition of the database engine. Logical operator is **Equals**. Possible values are: **Standard Edition**, **Standard Edition One**, **Standard Edition Two**, and **Enterprise Edition**.
- **License Pack**– The license pack. Logical operator is **Equals**. Possible values are: **Spatial and Graph**, **Active Data Guard**, **Label Security**, **Oracle On-Line Analytical Processing (OLAP)**, and **Diagnostic Pack and Tuning Pack**.

For more information, see Oracle Licensing in the *Amazon RDS User Guide*.

Adding automated discovery rules to a license configuration

After you add product information to your license configuration, License Manager can track license usage for the instances that have those products installed. For more information, see Automated discovery of resource inventory (p. 27).

To add automated discovery rules to a license configuration

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Open the **Search inventory** page.
3. Select the resource and choose **Add automated discovery rules**.
4. For **License configuration**, select a license configuration.
5. Specify the products to discover and track.
6. (Optional) Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
7. (Optional) To define resources to exclude from automated discovery select **Add exclusion rule**.

   Note
   Exclusion rules do not apply to RDS products (such as Oracle Database).

   a. Choose a **Property** to filter on, currently **Account ID**, and **Tag** are supported.
   b. Enter the information to identify that property. For an **Account ID** specify the 12 digit AWS Account ID as the value. For **Tags** enter a key/value pair.
   c. Repeat step 7 to add additional rules.
8. Choose **Add**.

Associating a license configuration with discovered inventory

After you have identified the unmanaged resources that you need to manage, you can manually associate them with a license configuration, instead of using automated discovery.

To associate a license configuration with a resource

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Open the **Search inventory** page.
3. Select the resource and choose **Associate license configuration**.

4. For **License configuration name**, select a license configuration.
5. (Optional) Select **Share license configuration with all my member accounts**.
6. Choose **Associate**.

Disassociating a license configuration and a resource

If the licensing terms from your software vendors change, you can disassociate resources that were associated manually and then delete the license configuration.

To disassociate a license configuration and a resource

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **License configuration**.
3. Choose the name of the license configuration.
4. Choose **Associated resources**.
5. Select each of the resources to disassociate from the license configuration and then choose **Disassociate resource**.

Automated discovery of resource inventory

License Manager uses Systems Manager inventory to discover software usage on Amazon EC2 instances and on-premises instances. You can add product information to your license configuration, and License Manager will track the instances that have those products installed. Additionally, you can specify exclusion rules based on your licensing agreement to decide which instances to exclude. You can exclude instances belonging to AWS account IDs or associated with resource tags from being considered for automated discovery

Automated discovery can be added to a new license set, to an existing license configuration, or resources in your inventory. Rules for automated discovery can be edited at any time through the CLI using the UpdateLicenseConfiguration API command. To edit rules in the console, you must delete the existing license configuration and create a new one.

To use automated discovery, you must add product information to your license configuration. You can do so when you create the license configuration using search inventory.

You cannot manually disassociate instances tracked by automated discovery. By default, automated discovery does not disassociate tracked instances after the software is uninstalled. You can configure automated discovery to stop tracking instances when the software is uninstalled.

After you configure automated discovery, you can track license usage through the License Manager dashboard.

Prerequisites

- Enable cross-account inventory discovery by integrating License Manager with your AWS Organizations account. For more information, see Settings in License Manager (p. 39).

  Note
  Single accounts can set up automated discovery but cannot add exclusion rules.
- Install Systems Manager inventory on your instances.

To configure automated discovery when you create a license configuration

You can configure automated discovery rules and exclusion rules when you create a license configuration. For more information, see Create a license configuration (p. 9).

To add automated discovery rules to an existing configuration

Use the process below to add automated discovery rules to existing license configurations through the console, you can also do this from the **Search inventory** pane by selecting an resource ID and selecting **Add automated discovery rules**.

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Customer managed licenses**.
3. Choose the name of the license configuration to open the license details page.
4. On the **Automated discovery rules** tab, choose **Add automated discovery rules**.
5. Specify the products to discover and track.
6. (Optional) Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
7. (Optional) To define resources to exclude from automated discovery select **Add exclusion rule**.

   Note
   Exclusion rules do not apply to RDS products (such as Oracle Database).

   a. Choose a **Property** to filter on, currently **Account ID**, and **Tag** are supported.
   b. Enter the information to identify that property. For an **Account ID** specify the 12 digit AWS account ID as the value. For **Tags** enter a key/value pair.
   c. Repeat step 7 to add additional rules.
8. When you are finished choose **Add** to apply your automated discovery rule.

Granted licenses in License Manager

Granted licenses are licenses for products that your organization purchased from AWS Marketplace, AWS Data Exchange, or directly from a seller who integrated their software with managed entitlements. License administrators can use AWS License Manager to govern the use of these licenses and to distribute rights of use, known as entitlements, to specific AWS accounts.

After a license administrator distributes an entitlement from an AWS Marketplace license to an AWS account, and the recipient accepts and activates the granted license, the subscription is available to the AWS account through AWS Marketplace. The account also has access to the product. For example, if a license administrator purchases an Amazon Machine Image (AMI) from AWS Marketplace and distributes an entitlement to your AWS account, you can launch Amazon EC2 instances from the AMI using AWS Marketplace and Amazon EC2.

Data licenses distributed to AWS Data Exchange products are available to the AWS account through AWS Data Exchange.

Before you can distribute licenses from AWS Marketplace, you must enable subscription sharing. For more information, see Sharing subscriptions in an organization.

Manage your granted licenses

After you purchase subscriptions from AWS Marketplace or AWS Data Exchange, purchase products from sellers that use License Manager to distribute licenses, or receive a grant from a license administrator, the granted licenses appear in the License Manager console. Recipients must accept and activate granted licenses before they can use the product.

How you accept and activate a license depends on whether the license is from AWS Marketplace, if your account is member account in an organization for AWS Organizations, and whether all features is enabled for your organization.

Granted licenses require cross-Region replication of license metadata. License Manager automatically replicates each granted license and its associated information to other Regions. This enables you to have a centralized view across all Regions where licenses are granted to you.

Licenses from AWS Marketplace and AWS Data Exchange

- Licenses for subscriptions that you purchase from AWS Marketplace are automatically accepted and activated.
- If the management account for an organization with all features enabled purchases a subscription from AWS Marketplace and distributes licenses to member accounts, the licenses are automatically accepted in the member accounts. Either the management account or the member accounts can later activate the license.
- If the management account for an organization with only consolidated billing features enabled purchases a subscription from AWS Marketplace and distributes licenses to member accounts, each member account must accept and activate the license.

Licenses from a seller

- You must accept and activate licenses for products that you purchase from a seller that uses License Manager to distribute licenses.
- If the management account for an organization with all features enabled purchases a product from a seller and distributes licenses to member accounts, the licenses are automatically accepted in the member accounts. Either the management account or the member accounts can later activate the license.
- If the management account for an organization with only consolidated billing features enabled purchases a product from a seller and distributes licenses to member accounts, each member account must accept and activate the license.

To manage your granted licenses

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. (Optional) Use the filter options, such as the following, to scope the list of licenses that are displayed.
   - Product name – The name of the product.
   - Issuer – The entity that issued the license. For example, licenses created by AWS Marketplace have an issuer of **AWS/Marketplace**.
   - Seller of record – The entity that sold the product.
   - Status – The status of the license. For example, **Available**.
   - Grant status – The status of the grant. For example, **Pending acceptance**.
4. To view additional information about the license, choose the license ID to open the license detail page.
5. If the license issuer is an entity other than AWS Marketplace, the initial grant status is **Pending acceptance**. Do one of the following:
   - Choose **Accept & activate license**. The resulting grant status is **Active**.
   - Choose **Accept license**. The resulting grant status is **Disabled**. When you are ready to use the license, choose **Activate license**.
   - Choose **Reject license**. The resulting grant status is **Rejected**. After you reject a license, you cannot activate it.
6. To stop using an active license, choose **Deactivate license**. When you are ready to use it again, choose **Activate license**.

To manage your granted licenses using the command line

- accept-grant (AWS CLI)
- create-grant-version (AWS CLI)
- get-grant (AWS CLI)
- list-licenses (AWS CLI)
- list-received-grants (AWS CLI)
- list-received-licenses (AWS CLI)
- reject-grant (AWS CLI)

Distribute an entitlement

If you are the license administrator, you can create a grant to distribute access to a license to another AWS account in your organization. You can create up to 2,000 grants per license.

To create a grant

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. Choose a license ID to open the license detail page.
4. From the **Grants** section, choose **Create grant**.
5. On the **Grant details** panel, do the following:
   a. Enter a name for the grant to help you identify the purpose or recipient of the grant.
   b. Enter the AWS account ID of the grant recipient.

      Note
      You can also enter the AWS Organizations ID for your organization to grant the entitlement to all accounts in your organization at once. For more information, see Distribution to AWS Organizations (p. 31).

   c. Choose **Create grant**.
6. When you return to the license detail page, you'll see an entry for the grant in the **Grants** panel. The initial status of the grant is **Pending acceptance**. The status changes to **Active** when the recipient accepts the grant or **Rejected** when the recipient rejects the grant.

To create a grant using the command line

- create-grant (AWS CLI)
- list-distributed-grants (AWS CLI)

Grant acceptance and activation

A granted license must be accepted and activated in the grantee account before it can be used.

By default, the grant details page for a granted license has a status of **Pending acceptance**. You can choose to **Accept**, **Accept and Activate**, or **Reject** the license.

Note
You can't activate two licenses for the same product from AWS Marketplace at the same time. If you have two subscriptions (for example, the public offer for a product and a private offer, or a subscribed license for a product and a granted license for the same product), you must deactivate the one that you are not using before you can activate the other.

Grants that are accepted but not yet activated have a status of **Disabled**. Accepted and activated grants have a status of **Active**.

> **Note**
> It is possible to have grants from the management account of your organization automatically accepted. To enable grant auto-acceptance, link your organization accounts via the AWS License Manager console settings from the management account.

Distribution to AWS Organizations

If you are a license administrator operating in the management account of an organization with all features enabled, you can distribute your licenses to all accounts in your organization at one time. To distribute your license to all accounts with one grant, choose your organization ID rather than a single account ID when distributing your entitlement. In the console, you can specify the organization ID or the organization ARN. Here is an example organization ARN: `arn:aws:organizations::<account-id-of-management-account>:organization/<organization-id>`. You must use the ARN when using the AWS License Manager API.

> **Note**
> In order to grant a license to your AWS Organizations ID, you must first link AWS Organizations accounts via the AWS License Manager console settings. For more information, see Settings in License Manager (p. 39).

The grant details page displays the list of accounts that you have granted access to the entitlement. After distributing a license to your organization, you can deactivate or activate the licenses individually on each account.

License status

Licenses have two statuses: The **License status**, which shows the overall availability and sharability of the license, and the **Grant status**, which shows the ability to use the license.

License statuses

Status	Description
Available	The license is available to use and share.
Deleted	The license is not available to use because the license agreement has been canceled.
Deactivated	The license it not available to use because it has been deactivated by the license issuer.
Expired	The license is not available to use because it has reached the end of term.

Grant statuses

Status	Description
Pending acceptance	The grant has been created and the grant recipient has not yet accepted it.
Disabled	The grant has been accepted by the recipient but has not been activated for use.

Status	Description
Active	The grant has been accepted and activated for use. The licensed resource can be used.
Rejected	The grant recipient has rejected the grant.
Deleted	The grantor has deleted the grant.
Workflow complete	The grant is a grant to an organization, and the workflow to distribute or recall the grant has been completed. The grant details show the status of sub-grants to each account in the organization.

Seller issued licenses in AWS License Manager

Independent software vendors (ISVs) can use AWS License Manager to manage and distribute software licenses to end users. As an issuer, you can track the usage of your seller issued licenses centrally using the License Manager dashboard.

License Manager uses open, secure, industry standards for representing licenses and allows customers to cryptographically verify their authenticity. License Manager associates each license with an asymmetric key. As the ISV, you own the asymmetric AWS KMS keys and store them in your account.

Seller issued licenses require cross-Region replication of license metadata. License Manager automatically replicates each seller issued license and its associated information to other Regions.

License Manager supports a variety of different licensing models including the following:

- **Perpetual** — Lifetime licenses with no expiration date that authorize users to use the software indefinitely.
- **Floating** - Shareable licenses with multiple instances of the application. Licenses can be prepaid and a fixed set of entitlements added to them.
- **Subscription** - Licenses with expiration dates that can be automatically renewed unless specifically deactivated.
- **Usage-based** - Licenses with specific terms based on usage, such as the number of API requests, transactions, or storage capabilities.

You can create licenses in License Manager and distribute them to customers using an AWS IAM identity or through bearer tokens generated by License Manager. Customers with an AWS account can re-distribute the license entitlements to AWS identities in their respective organizations. Customers with distributed entitlements can check out and check in the required entitlements from that license through your software integration with License Manager.

Entitlements

License Manager captures license capabilities as *entitlements* in the license. Entitlements can be characterized with a limited or unlimited quantity. An example of a limited entitlement is ‘40 GB of data transfer’. An example of an unlimited quantity entitlement is ‘Platinum Tier’.

A license captures all the granted entitlements, the activation and expiration dates, and the issuer details. A license is a versioned entity and each version is immutable. License versions are updated whenever the license is changed.

To check out or check in limited entitlements, ISV applications must specify the amount of each limited capacity. For unlimited entitlements, ISV applications can simply specify the relevant entitlement to check out or check in again. Finally, limited capabilities also support an “overage” flag, which indicates if end-users can exceed their usage of the initial entitlements. License Manager tracks and reports usage, along with any overages, to the ISV.

License usage

License Manager allows you to centrally track licenses across multiple Regions, by maintaining a count of all the checked out entitlements. License Manager also tracks the identity of the user and the underlying resource identifier, if available, associated with each check out, along with when it was checked out. You can track this time-series data through CloudWatch Events.

Licenses may be in one of the following states:

- **Created** - The license is created.
- **Updated** - The license is updated.
- **Deactivated** - The license is deactivated.
- **Deleted** - The license is deleted.

Requirements

To get started with this feature, you need permission to call the following License Manager API actions.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenses",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:GetLicenseUsage",
            "license-manager:CreateGrant",
            "license-manager:CreateGrantVersion",
            "license-manager:DeleteGrant",
            "license-manager:GetGrant",
            "license-manager:ListDistributedGrants"
        ],
        "Resource": "*"
      }
    ]
}
```

If you will integrate with License Manager so customers without an AWS account can consume licenses sold outside of AWS Marketplace, you must create a role that enables your software application to call the License Manager API. For example, you can use the AWS CLI. First, use the create-role command to create a role named **AWSLicenseManagerConsumptionRole**.

```
aws iam create-role
```

```
    --role-name AWSLicenseManagerConsumptionRole
    --description "Role used to consume licenses using AWS License Manager"
    --max-session-duration 3600
    --assume-role-policy-document file://trust-policy-document.json
```

The following is `trust-policy-document.json`.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Federated": "openid-license-manager.amazonaws.com"
        },
        "Action": "sts:AssumeRoleWithWebIdentity",
        "Condition": {
            "StringLike": {
                "openid-license-manager.amazonaws.com:sub": "66a9bbf5-0896-460f-a1a9-
de535dcc175b"
            }
        }
    }
}
```

Next, use the attach-role-policy command to add the **AWSLicenseManagerConsumptionPolicy** AWS managed policy to the **AWSLicenseManagerConsumptionRole** role.

```
aws iam attach-role-policy
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy
    --role-name AWSLicenseManagerConsumptionRole
```

Creating seller issued licenses

Use the following procedure to create a block of licenses to grant to customers using the AWS Management Console. Alternatively, you can create the license using the CreateLicense API action.

To create a license using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Seller Issued Licenses** from the left menu.
3. Choose **Create license**.
4. For **License metadata**, provide the following information:
   - **License name** - The name, up to 150 characters, to display to buyers.
   - **License description** - An optional description, up to 400 characters, that differentiates this license from other licenses.
   - **Product SKU** - The product SKU.
   - **Recipient** - The recipient's name (company or individual).
   - **Home Region** - The AWS Region for the license. Although licenses can be consumed globally, you can only change the license in the home region. You cannot change the home region for a license after you create it.
   - **License start date** - The date of activation.
   - **License end date** - The end date of the license, if applicable.
5. For **Consumption configuration**, provide the following information:
   - **Renewal frequency** - Whether to renew weekly, monthly, or not at all.

- **Consumption configuration** - Choose **Provisional Consumption Configuration Options** if the license is to be used for continuous connectivity or **Borrow** if the license is to be used offline. Enter **Max time to live (minutes)** to set the length of availability of the license.

6. For **Issuer**, provide the following information:

   - **Enter an AWS KMS key** - License Manager uses this key to sign and verify the issuer. For more information, see Cryptographic Signing of Licenses (p. 54).
   - **Issuer name** - The business name for the seller.
   - **Seller of record** - An optional business name.
   - **Agreement URL** - The URL to the license agreement.

7. For **Entitlement**, provide the following information about the capabilities that the license grants to recipients:

   - **Name** - The name of the recipient.
   - **Unit type** - Select the unit type, then provide the maximum count.
   - Check **Allow check in** if recipients must check in licenses before renewal.
   - Check **Overages allowed** if recipients can use the resource beyond the maximum count. This option might incur additional charges for the recipient.

8. Choose **Create license**.

Granting licenses to customers

After you add the new license, you can grant the license to a customer with an AWS account using the AWS Management Console. The recipient must accept the grant before using the license. For more information, see Granted licenses in License Manager (p. 28).

Alternatively, if the customer does not have an AWS account, you can use the License Manager API to enable customers to consume licenses (p. 36).

To grant a license to a customer using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Seller Issued Licenses** from the left menu.
3. Choose the ID of the license to open its details page.
4. For **Grants**, choose **Create grant**.
5. For **Grant details**, provide the following information:

   - **Grant name** - The grant name. This is used to enable search capabilities.
   - **AWS account ID** - The AWS account number of the license recipient.
   - **License rights** - Choose **Consumption** if the recipient can consume granted entitlements only and **Distribution** if the recipient can distribute granted entitlements to other AWS accounts.
   - **Home Region** - The AWS Region for the license.

6. Choose **Create grant**.

Getting temporary credentials for customers without an AWS account

If you have customers that do not have an AWS account, you can use entitlements for them the same way that you do for your customers with an AWS account. Use the following procedure to get temporary

AWS credentials for your customers without an AWS account. The API calls must be made in the home Region.

To get temporary credentials to use in calling the License Manager API

1. Call the CreateToken API action to get a refresh token encoded as a JWT token.
2. Call the GetAccessToken API action, specifying the refresh token that you received from `CreateToken` in the previous step, to receive a temporary access token.
3. Call the AssumeRoleWithWebIdentity API action, specifying the access token that you received from `GetAccessToken` in the previous step, and the **AWSLicenseManagerConsumptionRole** role that you created, to get temporary AWS credentials.

Consuming licenses

License Manager allows multiple users to concurrently consume entitlements, with limited capabilities, from a single license. Call the CheckoutLicense API action. The following is a description of the parameters.

- **Key fingerprint** — Trusted license issuer.

  Example: aws:123456789012:issuer:issuer-fingerprint
- **Product SKU** — Product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs. Therefore, trusted key fingerprints play an important role.

  Example: 1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE
- **Entitlements** — Capabilities to check out. If you specify an unlimited capability, the quantity is zero. Example:

```
"Entitlements": [
    {
        "Name": "DataTransfer",
        "Unit": "Gigabytes",
        "Value": 10
    },
    {
        "Name": "DataStorage",
        "Unit": "Gigabytes",
        "Value": 5
    }
]
```

- **Beneficiary** — Software as a Service (SaaS) ISVs can check out licenses on behalf of a customer by including the customer identifier. License Manager limits the call to the repository of licenses created in the SaaS ISV account.

  Example: user@domain.com
- **Node ID** — An identifier used to node-lock the license to a single instance of the application.

  Example: 10.0.21.57

Deleting seller issued licenses

After you delete a license, you can recreate it. The license and its data are retained and available to the license issuer and license grantees in read-only mode for six months.

Use the following procedure to delete a license that you have created using the AWS Management Console. Alternatively, you can delete the license using the DeleteLicense API action.

To delete a license using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Seller issued licenses** from the left menu.
3. Choose the radio button next to the license to select it for deletion.
4. Choose **Delete**. When prompted for confirmation, enter **`delete`** and choose **Delete**.

Register a delegated administrator

You can delegate a member account from your organization to perform administrative tasks, such as sharing license configurations with other member accounts, performing cross-account resource discovery, and distributing managed entitlements to other member accounts. Only member accounts that are part of your AWS Organizations can be registered as a delegated administrator. For more information about joining an organization, see Inviting an AWS account to join your organization.

Your can register one delegated administrator per organization. Before you register a delegated administrator, you must enable trusted access with AWS Organizations. For more information, see Enable trusted access with AWS Organizations.

> **Important**
> Once registered, the delegated administrator has visibility into EC2 instances owned by accounts in your organization.

The following AWS Regions support License Manager delegated administrators:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Hong Kong)
- Middle East (Bahrain)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Africa (Cape Town)
- South America (São Paulo)
- AWS GovCloud (US-East)

- AWS GovCloud (US-West)

You can register and deregister delegated administrators using the AWS License Manager console, AWS CLI, or AWS SDKs.

Delegated administration topics

Register a delegated administrator (console)

To register a delegated administrator using the AWS License Manager console, perform the following steps:

1. Sign in to AWS as the administrator of the management account.
2. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
3. Choose **Settings** from the left navigation pane.
4. Under **Delegated administrators**, choose **Delegate administrator**.
5. To register a delegated administrator, enter the account ID and select **Delegate**.
6. A message indicates that the specified account has been successfully registered as a delegated administrator.

Deregister a delegated administrator (console)

To deregister a delegated administrator using the AWS License Manager console, perform the following steps:

1. Sign in to AWS as the administrator of the management account.
2. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
3. Choose **Settings** from the left navigation pane.
4. Under **Delegated adminstrators**, choose **Remove**.
5. Verify successful deregistering of delegated administrator by choosing **Remove** again.

Register a delegated administrator (AWS CLI)

To register a delegated administrator using the AWS CLI, perform the following steps:

1. From the command line, run the following AWS CLI command:

```
aws organizations register-delegated-administrator --service-principal=license-
manager.amazonaws.com --account-id=<account-id>
```

2. Run the following command to verify that the specified account is successfully registered as the delegated administrator:

```
aws organizations list-delegated-administrators  --service-principal=license-
manager.amazonaws.com
```

Deregister a delegated administrator (AWS CLI)

To deregister a delegated administrator using the AWS CLI, perform the following steps:

1. From the command line, run the following AWS CLI command:

```
aws organizations deregister-delegated-administrator --service-principal=license-
manager.amazonaws.com --account-id=<account-id>
```

2. Run the following command to verify that the specified account is successfully deregistered as the delegated administrator:

```
aws organizations list-delegated-administrators  --service-principal=license-
manager.amazonaws.com
```

You can register a deregistered account again at any time.

Settings in License Manager

The **Settings** section of the License Manager console displays settings for the logged-in account. You must configure settings to enable distribution of managed entitlements and license configurations to your organization, as well as for performing cross-account inventory discovery.

The settings for License Manager include the following:

- **Account type**
- **S3 bucket ARN**
- **Link AWS Organizations account** status
- **SNS topic ARN**
- **Cross-account resource discovery**
- **Resource share ARN**
- **Register/De-register Delegated Admin** (if applicable)

To edit License Manager settings

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Settings**.
3. Choose **Edit**.

Enable distribution of managed entitlements or license configurations to your organization

To distribute managed entitlements or license configurations within your organization, select the check box next to **Link AWS Organizations accounts**. The distributed grants for managed entitlements are auto-accepted by all of your member accounts. When you select this option, we add a service-linked role to the management (p. 47) and member (p. 50) accounts.

> **Note**
> To enable this option, you must be signed in to your management account and all features must be enabled in AWS Organizations. For more information, see Enabling all features in your organization in the *AWS Organizations User Guide*.

This selection also creates an AWS Resource Access Manager resource share in your management account, which allows you to seamlessly share license configurations. For more information, see the AWS Resource Access Manager User Guide.

To disable this option, call the UpdateServiceSettings API.

Perform cross-account resource discovery in your AWS Organizations

To enable cross-account resource discovery in your Organizations, select the check box next to **Turn on cross-account inventory search**. When you turn on the cross-account inventory search, your AWS Organizations will automatically be linked to perform inventory search across all of your accounts.

Note
License Manager uses Systems Manager inventory to discover software usage. Verify that you have configured Systems Manager inventory on all of your resources. Querying Systems Manager inventory requires the following:

- Resource data sync to store inventory in an Amazon S3 bucket.
- Amazon Athena to aggregate inventory data from organizational accounts.
- AWS Glue to provide a fast query experience.

(Optional) For Amazon Simple Notification Service, edit the **Amazon SNS topic ARN**. The ARN must use the following format:

```
arn:<aws_partition>:sns:region:account_id:aws-license-manager-service-*
```

Dashboard in License Manager

The **Dashboard** section of the AWS License Manager console provides graphs to track the license consumption associate with each license configuration. The dashboard also displays alerts resulting from license rule violations.

The following information is available in the graph for a license configuration:

- License configuration name
- License type
- Licenses consumed
- Number of licenses remaining
- Whether the rules are enforced
- Number of hosts for each tenancy type

Security in AWS License Manager

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to License Manager, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using License Manager. It shows you how to configure License Manager to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your License Manager resources.

Contents

Data protection in AWS License Manager

The AWS shared responsibility model applies to data protection in AWS License Manager. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.

- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with License Manager or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption at rest

License Manager stores data in an Amazon S3 bucket in the management account. The bucket is configured using Amazon S3 managed encryption keys (SSE-S3).

Identity and access management for AWS License Manager

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use AWS resources. With IAM you can create users and groups under your AWS account. You control the permissions that users have to perform tasks using AWS resources. You can use IAM for no additional charge.

By default, IAM users don't have permissions for License Manager resources and operations. To allow IAM users to manage License Manager resources, you must create an IAM policy that explicitly grants them permissions. Then you attach the policy to the IAM users or groups that require those permissions.

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources. For more information, see Policies and Permissions in the *IAM User Guide* guide.

Policy structure

An IAM policy is a JSON document that consists of one or more statements. Each statement is structured as follows.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Various elements make up a statement:

- **Effect:** The *effect* can be `Allow` or `Deny`. By default, IAM users don't have permission to use resources and API operations, so all requests are denied. An explicit *allow* overrides the default. An explicit *deny* overrides any allows.
- **Action**: The *action* is the specific API operation for which you are granting or denying permission.
- **Resource**: The resource is affected by the action. Some License Manager API operations allow you to include specific resources in your policy that can be created or modified by the operation. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN). For more information, see Actions Defined by AWS License Manager.
- **Condition**: Conditions are optional. They can be used to control when your policy is in effect. For more information, see Condition Keys for AWS License Manager.

Policy for an ISV using License Manager

ISVs that distribute licenses through License Manager require the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:ListLicenses",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
            "license-manager:CheckInLicense",
            "kms:GetPublicKey"
        ],
        "Resource": "*"
        }
    ]
}
```

Example policies for License Manager

In an IAM policy statement, you can specify any API operation from any service that supports IAM. For License Manager, use the following prefix with the name of the API operation: `license-manager:`. For example:

- `license-manager:CreateLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`

To specify multiple operations in a single statement, separate them with commas as follows:

```
"Action": ["license-manager:action1", "license-manager:action2"]
```

You can also specify multiple operations using wildcards. For example, you can specify all License Manager API operations whose name begins with the word *List* as follows:

```
"Action": "license-manager:List*"
```

To specify all License Manager API operations, use the * wildcard as follows:

```
"Action": "license-manager:*"
```

Using service-linked roles for AWS License Manager

AWS License Manager 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 License Manager. Service-linked roles are predefined by License Manager and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up License Manager easier because you don't have to manually add the necessary permissions. License Manager defines the permissions of its service-linked roles, and unless defined otherwise, only License Manager 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 the related resources. This protects your License Manager resources because you can't inadvertently remove permissions to access the resources.

License Manager actions depend on three service-linked roles, as described in the following sections.

Service-linked roles

License Manager—Core role

License Manager requires a service-linked role to manage licenses on your behalf.

Permissions for the core role

The service-linked role named **AWSServiceRoleForAWSLicenseManagerRole** allows License Manager access to AWS resources to manage licenses on your behalf.

The **AWSServiceRoleForAWSLicenseManagerRole** service-linked role trusts the `license-manager.amazonaws.com` service to assume the role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
`iam:CreateServiceLinkedRole`	`arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManage`

Action	Resource ARN
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberA
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

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*.

Create a service-linked role for License Manager

You don't need to manually create a service-linked role. When you complete the License Manager first-run experience form the first time that you visit the License Manager console, the service-linked role is automatically created for you.

You can also use the IAM console, AWS CLI, or IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using License Manager before January 1, 2017, when it began supporting service-linked roles, then License Manager created the **AWSServiceRoleForAWSLicenseManagerRole** role in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create a service-linked role.

To create a service-linked role

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Start using License Manager**.
3. In the **IAM Permissions (one-time-setup)** form, select **I grant AWS License Manager the required permissions**, then choose **Continue**.

You can also use the IAM console to create a service-linked role with the **License Manager** use case. Alternatively, in the AWS CLI or the AWS API, use IAM to create a service-linked role with the `license-manager.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 the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager does not allow you to edit the **AWSServiceRoleForAWSLicenseManagerRole** 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*.

Delete a service-linked role for License Manager

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 only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Clean up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete all resources used by the role. This means disassociating any license configurations from associated instances and AMIs, and then deleting the license configurations.

> **Note**
> If License Manager 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 action again.

To delete License Manager resources used by the core role

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **License configuration**.
3. For a specific license configuration for which you are the owner, disassociate all associated AMIs and resources.
4. While still on the license configuration page, delete the license configuration.
5. Repeat the previous steps until all license configurations have been deleted.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the **AWSServiceRoleForAWSLicenseManagerRole** service-linked role. If you are also using AWSLicenseManagerMasterAccountRole (p. 47) and AWSLicenseManagerMemberAccountRole (p. 50), delete those roles first. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

License Manager–Management account role

License Manager requires a service-linked role to perform license management.

Permissions for the management account role

The service-linked role named **AWSServiceRoleForAWSLicenseManagerMasterAccountRole** allows License Manager access to AWS resources to manage license management actions for a central management account on your behalf.

The **AWSServiceRoleForAWSLicenseManagerMasterAccountRole** service-linked role trusts the `license-manager.master-account.amazonaws.com` service to assume the role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
`s3:GetBucketLocation`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:ListBucket`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:GetLifecycleConfiguration`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:PutLifecycleConfiguration`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:GetBucketPolicy`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:PutBucketPolicy`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:AbortMultipartUpload`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:PutObject`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:GetObject`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:ListBucketMultipartUploads`	`arn:aws:s3:::aws-license-manager-service-*`
`s3:ListMultipartUploadParts`	`arn:aws:s3:::aws-license-manager-service-*`

Action	Resource ARN
s3:DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram:DeleteResourceShare	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

Action	Resource ARN
`cloudformation:DeleteStack`	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
`cloudformation:DescribeStacks`	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
`glue:CreateTable`	See footnote †
`glue:UpdateTable`	See footnote †
`glue:DeleteTable`	See footnote †
`glue:UpdateJob`	See footnote †
`glue:UpdateCrawler`	See footnote †

† The following are the conditions for the AWS Glue actions:

- `arn:aws:glue:*:*:catalog`
- `arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler`
- `arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob`
- `arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*`
- `arn:aws:glue:*:*:table/license_manager_resource_sync/*`
- `arn:aws:glue:*:*:database/license_manager_resource_inventory_db`
- `arn:aws:glue:*:*:database/license_manager_resource_sync`

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*.

Create a management account service-linked role

You don't need to manually create this service-linked role. When you configure cross-account license management in the AWS Management Console, License Manager creates the service-linked role for you.

> **Note**
> To make use of cross-account support in License Manager, you must be using AWS Organizations.

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.

You can also use the IAM console, AWS CLI, or IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using License Manager before January 1, 2017, when it began supporting service-linked roles, then License Manager created **AWSServiceRoleForAWSLicenseManagerMasterAccountRole** in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create this service-linked role.

To create the service-linked role

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Choose **Settings**, **Edit**.
3. Choose **Link AWS Organizations accounts**.
4. Choose **Apply**.

You can also use the IAM console to create a service-linked role with the **License Manager**–Management account use case. Alternatively, in the AWS CLI or the AWS API, use IAM to create a service-linked role with the `license-manager.master-account.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 the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager does not allow you to edit the **AWSServiceRoleForAWSLicenseManagerMasterAccountRole** 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*.

Delete a service-linked role for License Manager

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 only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Manually delete the service-linked role

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

License Manager–Member account role

License Manager requires a service-linked role that allows the management account to manage licenses.

Permissions for the member account role

The service-linked role named **AWSServiceRoleForAWSLicenseManagerMemberAccountRole** allows License Manager to access AWS resources for license management actions from a configured management account on your behalf.

The **AWSServiceRoleForAWSLicenseManagerMemberAccountRole** service-linked role trusts the `license-manager.member-account.amazonaws.com` service to assume the role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
`license-manager:UpdateLicenseSpecificationsForResource`	*

Action	Resource ARN
license-manager:GetLicenseConfiguration	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:CreateResourceDataSync	*
ssm:DeleteResourceDataSync	*
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

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*.

Create the service-linked role for License Manager

You don't need to manually create the service-linked role. You can enable integration with AWS Organizations from the management account in the License Manager console on the **Settings** page. You can also do this using the AWS CLI (run `update-service-settings`) or the AWS API (call `UpdateServiceSettings`). When you do, License Manager creates the service-linked role for you in the Organizations member accounts.

If you delete this service-linked role and then need to create it again, you can use the same process to recreate the role in your account.

You can also use the IAM console, AWS CLI, or IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using the License Manager service before January 1, 2017, when it began supporting service-linked roles, then License Manager created the **AWSServiceRoleForAWSLicenseManagerMemberAccountRole** role in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create a service-linked role.

To create a service-linked role

1. Log into your AWS Organizations management account.
2. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
3. In the left navigation pane, choose **Settings**, **Edit**.
4. Choose **Link AWS Organizations accounts**.
5. Choose **Apply**. This creates the roles AWSServiceRoleForAWSLicenseManagerRole (p. 44) and AWSServiceRoleForAWSLicenseManagerMemberAccountRole (p. 50) in all child accounts.

You can also use the IAM console to create a service-linked role with the **License Manager - Member account** use case. Alternatively, in the AWS CLI or AWS API, create a service-linked role with the `license-manager.member-account.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 the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager does not allow you to edit the **AWSServiceRoleForAWSLicenseManagerMemberAccountRole** 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*.

Delete a service-linked role for License Manager

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 only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Manually delete the service-linked role

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

AWS managed policies for AWS License Manager

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AWSLicenseManagerServiceRolePolicy

This policy is attached to the service-linked role named **AWSServiceRoleForAWSLicenseManagerRole** to allow License Manager to call API actions to manage licenses on your behalf. For more information, see Using service-linked roles for AWS License Manager (p. 44).

AWS managed policy: AWSLicenseManagerMasterAccountRolePolicy

This policy is attached to the service-linked role named **AWSServiceRoleForAWSLicenseManagerMasterAccountRole** to allow License Manager to call API actions to manage license management for a central management account on your behalf. For more information, see Using service-linked roles for AWS License Manager (p. 44).

AWS managed policy: AWSLicenseManagerMemberAccountRolePolicy

This policy is attached to the service-linked role named **AWSServiceRoleForAWSLicenseManagerMemberAccountRole** to allow License Manager to call API actions for license management from a configured management account on your behalf. For more information, see Using service-linked roles for AWS License Manager (p. 44).

AWS managed policy: AWSLicenseManagerConsumptionPolicy

You can attach the `AWSLicenseManagerConsumptionPolicy` policy to your IAM identities. This policy grants permissions that allow access to the License Manager API actions required to consume licenses. For more information, see License usage (p. 33).

To view the permissions for this policy, see AWSLicenseManagerConsumptionPolicy in the AWS Management Console.

License Manager updates to AWS managed policies

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

Change	Description	Date
AWSLicenseManagerConsumptionPolicy (p. 53) - New policy	License Manager added a new policy that grants permissions to consume licenses.	Aug 11, 2021
AWSLicenseManagerServiceRolePolicy (p. 52) - Update to an existing policy	License Manager added a permission to list delegated administrators and a permission to create the service-linked role named **AWSServiceRoleForAWSLicenseManagerMemberAccountRole**.	June 16, 2021
AWSLicenseManagerServiceRolePolicy (p. 52) - Update to an existing policy	License Manager added a permission to list all License Manager resources, such as license configurations, licenses, and grants.	June 15, 2021

Change	Description	Date
AWSLicenseManagerServiceRolePolicy (p. 52) - Update to an existing policy	License Manager added a permission to create the service-linked role named **AWSServiceRoleForMarketplaceLicenseManagement**. This role provides AWS Marketplace with permissions to create and manage licenses in License Manager. For more information, see Service-linked roles for AWS Marketplace in the *AWS Marketplace Buyer Guide*.	March 9, 2021
License Manager started tracking changes	License Manager started tracking changes to its AWS managed policies.	March 9, 2021

Cryptographic Signing of Licenses

License Manager can cryptographically sign licenses issued by an ISV or through AWS Marketplace on behalf of an ISV. Signing permits vendors to validate the integrity and origin of a license within the application itself, even in an offline environment.

To sign licenses, License Manager uses an asymmetric customer master key (CMK) belonging to an ISV and protected in AWS Key Management Service (AWS KMS). This customer managed CMK consists of a mathematically related public key and private key pair. When a user requests a license, License Manager generates a JSON object listing the license entitlements, and signs this object with the private key. The signature and the plaintext JSON object are returned to the user. Any party presented with these objects can use the public key to validate that the text of the license has not been altered and that the license was signed by the owner of the private key. The private part of the key pair never leaves AWS KMS. For more information about asymmetric cryptography in AWS KMS, see Using symmetric and asymmetric keys.

> **Note**
> License Manager calls the AWS KMS `Sign` and `Verify` API operations when signing and verifying licenses. The CMK must have a key usage value of SIGN_VERIFY for it to be used by these operations. This variety of CMK cannot be used for encryption and decryption.

The following workflow describes the issuance of cryptographically signed licenses:

1. In the AWS KMS console, API, or SDK, the license administrator creates an asymmetric customer managed CMK. The CMK must have a key usage of sign and verify, and support the RSASSA-PSS SHA-256 signing algorithm. For more information, see Creating asymmetric CMKs and How to choose your CMK configuration.
2. In License Manager, the license administrator creates a consumption configuration that includes an AWS KMS ARN or ID. The configuration may specify either or both the **Borrow** and **Provisional** options. For more information, see Creating a block of seller issued licenses.
3. An end-user obtains the license using the `CheckoutLicense` or `CheckoutBorrowLicense` API operation. The `CheckoutBorrowLicense` operation is allowed only on licenses with **Borrow** configured. It returns a digital signature as part of its response along with the JSON object listing entitlements. The plaintext JSON resembles the following:

```
{
   "entitlementsAllowed":[
      {
```

```
         "name":"EntitlementCount",
         "unit":"Count",
         "value":"1"
      }
   ],
   "expiration":"2020-12-01T00:47:35",
   "issuedAt":"2020-11-30T23:47:35",
   "licenseArn":"arn:aws:license-
manager::277886486208:license:l-6585590917ad46858328ff02dEXAMPLE",
   "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
   "nodeId":"100.20.15.10",
   "checkoutMetadata":{
      "Mac":"ABCDEFGHI"
   }
}
```

Compliance validation for AWS License Manager

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether AWS License Manager or other AWS services are in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance Whitepaper – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

  Note
  Not all services are compliant with HIPAA.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in AWS License Manager

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate

applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in AWS License Manager

As a managed service, AWS License Manager is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access License Manager through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

AWS License Manager and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your virtual private cloud (VPC) and AWS License Manager by creating an interface VPC endpoint. Interface endpoints are powered by AWS PrivateLink, a technology that you can use to privately access the License Manager API without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with License Manager. Traffic between your VPC and License Manager does not leave the Amazon network.

Each interface endpoint is represented by one or more Elastic Network Interfaces in your subnets.

For more information, see Interface VPC endpoints (AWS PrivateLink) in the *Amazon VPC User Guide*.

Create an interface VPC endpoint for License Manager

Create an interface endpoint for License Manager using one of the following service names:

- **com.amazonaws.*region*.license-manager**
- **com.amazonaws.*region*.license-manager-fips**

If you enable private DNS for the endpoint, you can make API requests to License Manager using its default DNS name for the Region. For example, `license-manager.region.amazonaws.com`.

For more information, see Creating an Interface Endpoint in the *Amazon VPC User Guide*.

Create a VPC endpoint policy for License Manager

You can attach a policy to your VPC endpoint to control access to License Manager. The policy specifies the following information:

- The principal that can perform actions
- The actions that can be performed
- The resource on which the actions can be performed

The following is an example of an endpoint policy for License Manager. When attached to an endpoint, this policy grants access to the specified License Manager actions for all principals on all resources.

```
{
   "Statement": [
        {
            "Principal": "*",
            "Effect": "Allow",
            "Action": [
              "license-manager:*"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Controlling access to services using VPC endpoints in the *Amazon VPC User Guide*.

Troubleshooting AWS License Manager

The following information can help you troubleshoot issues when using AWS License Manager. Before you start, confirm that your License Manager setup meets the requirements stated in Settings in License Manager (p. 39).

Cross-account discovery error

While setting up cross-account discovery, you may encounter the following error message on the **Search Inventory** page:

Athena Exception: Athena Query failed because - Insufficient permissions to execute the query. Please migrate your Catalog to enable access to this database.

This can occur if your Athena service uses the Athena-managed data catalog rather than the AWS Glue Data Catalog. For upgrade instructions, see Upgrading to the AWS Glue Data Catalog Step-by-Step.

Master account cannot disassociate resources from a license Configuration

If a member account of an Organization deletes the `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` Service Linked Role (SLR) in its account, and there are member-owned resources associated with a license configuration, the management account is prevented from disassociating licenses from those member-account resources. This means that the member account resources will continue to consume licenses from the management account pool. To allow the management account to disassociate resources, restore the SLR.

This behavior accounts for cases when a customer prefers not to allow the management account to perform some actions affecting member-account resources.

Systems Manager Inventory is out of date

Systems Manager stores data in its Inventory data for 30 days. During this period, License Manager counts a managed instance as active even if it is not pingable. After inventory data has been purged from Systems Manager, License Manager marks the instance as inactive and updates local inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in Systems Manager so that License Manager can run cleanup operations.

Apparent persistence of a de-registered AMI

License Manager purges stale associations between resources and license configurations once every few hours. If an AMI associated with a license configuration is deregistered through Amazon EC2, The AMI may briefly continue to appear in the License Manager resource inventory before being purged.

New child account instances are slow to appear in resource inventory

When cross-account support is enabled, License Manager updates customer accounts at 1 PM daily by default. Instances added later in the day show up in the management account resource inventory on the following day. You can change the frequency at which the update script runs by editing the `LicenseManagerResourceSynDataProcessJobTrigger` in the AWS Glue console for the management account.

After enabling cross-account mode, child account instances are slow to appear

When you enable cross-account mode in License Manager, instances in child accounts may take anywhere from a few minutes to a few hours to appear in the resource inventory. The time depends on the number of child accounts and the number of instances in each child account.

Cross-account discovery cannot be disabled

After an account is configured for cross-account discovery, it is impossible to revert to single-account discovery.

Child account user cannot associate shared license configuration with an instance

When this occurs and cross-account discovery has been enabled, check for the following:

- The child account has been removed from the organization.
- The child account has been removed from the resource share created in the management account.
- The license configuration has been removed from the resource share.

Linking AWS Organizations accounts fails

If the **Settings** page reports this error, it means that an account is not a member of an organization for the following reasons:

- A child account was removed from the organization.
- A customer turned off access to License Manager from organization console of the management account.

Logging AWS License Manager API calls using AWS CloudTrail

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

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

License Manager information in CloudTrail

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

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

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All License Manager actions are logged by CloudTrail and are documented in the License Manager API Reference. For example, calls to the `CreateLicenseConfiguration`, `ListResourceInventory` and `DeleteLicenseConfiguration` actions generate entries in the CloudTrail log files.

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

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

For more information, see the CloudTrail userIdentity Element.

Understanding License Manager log file entries

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

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


```
{
   "eventVersion":"1.05",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDAIF2U5EXAMPLEH5AP6",
      "arn":"arn:aws:iam::012345678901:user/Administrator",
      "accountId":"012345678901",
      "accessKeyId":"AKIDEXAMPLE",
      "userName":"Administrator"
   },
   "eventTime":"2019-02-15T06:48:37Z",
   "eventSource":"license-manager.amazonaws.com",
   "eventName":"DeleteLicenseConfiguration",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.83",
   "userAgent":"Coral/Netty4",
   "requestParameters":{
      "licenseConfigurationArn":"arn:aws:license-manager:us-east-1:012345678901:license-
configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
   },
   "responseElements":null,
   "requestID":"3366df5f-4166-415f-9437-c38EXAMPLE48",
   "eventID":"6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
   "eventType":"AwsApiCall",
   "recipientAccountId":"012345678901"
}
```

Document history for AWS License Manager

The following table describes the releases of AWS License Manager.

Feature	Description	Date
License type conversion	Change your license type between AWS-provided licensing and Bring Your Own License (BYOL) without redeploying your existing workloads..	September 22, 2021
Sharing entitlements	Share managed license entitlements with your entire organization with one request.	July 16, 2021
License reports	Track the history of your license type configurations with License Manager report generators.	May 18, 2021
Automated discovery exclusion rules	Exclude instances from License Manager automated discovery based on AWS account IDs and tags.	March 5, 2021
Managed entitlements	Track and distribute license entitlements for products purchased from AWS Marketplace and sellers who use License Manager to distribute licenses.	December 3, 2020
Automated accounting for uninstalled software	Configure automated discovery to stop tracking instances when software is uninstalled.	December 3, 2020
Tag-based filtering	Search your resource inventory using tags.	December 3, 2020
AMI association scope	Associate your license configurations and the AMIs shared with your AWS account.	November 23, 2020
License affinity to host	Enforce license assignment to dedicated hardware for a specific number of days.	August 12, 2020
Track Oracle deployments on Amazon RDS	Track license usage for Oracle database engine editions and licensing packs on Amazon RDS.	March 23, 2020

Feature	Description	Date
Host resource groups	Configure a host resource group to enable License Manager to manage your Dedicated Hosts.	December 1, 2019
Automated software discovery	Configure License Manager to search for newly installed operating systems or applications and attach the corresponding license configurations to the instances.	December 1, 2019
Differentiate between license included and bring your own license	Filter your search results based on whether you are using licenses provided by Amazon or your own licenses.	November 8, 2019
Attach licenses to on-premises resources	After you attach licenses to an on-premises instance, License Manager periodically collects software inventory, updates licensing information, and reports usage.	March 8, 2019
AWS License Manager initial release	Initial service launch	November 28, 2018