AWS License Manager

User Guide

AWS License Manager: User Guide

Table of Contents

What Is AWS License Manager?

AWS License Manager streamlines the process of bringing software vendor licenses to the cloud. As you build out cloud infrastructure on AWS, you can save costs by using bring-your-own-license (BYOL) opportunities, that is, by repurposing your existing license inventory for use with 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, stopping non-compliant server usage before it happens. A reporting dashboard provides ongoing visibility into license usage and assists with vendor audits.

License Manager helps you manage licenses for the following:

- AWS Cloud resources
- On-premises resources

License Manager currently integrates with Amazon EC2, allowing you to track licenses for default (shared-tenancy) EC2 instances, Dedicated Instances, Dedicated Hosts, Spot Instances and Spot Fleet, Systems Manager Managed Instances, and Auto Scaling groups. You can use License Manager with AWS Systems Manager to manage licenses for on-premises servers and non-AWS public clouds. You can also use it with AWS Organizations to manage all of your organizational accounts centrally.

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.

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

Using License Manager along with Amazon EC2 Systems Manager, you can manage licenses on physical or virtual servers hosted outside of AWS.

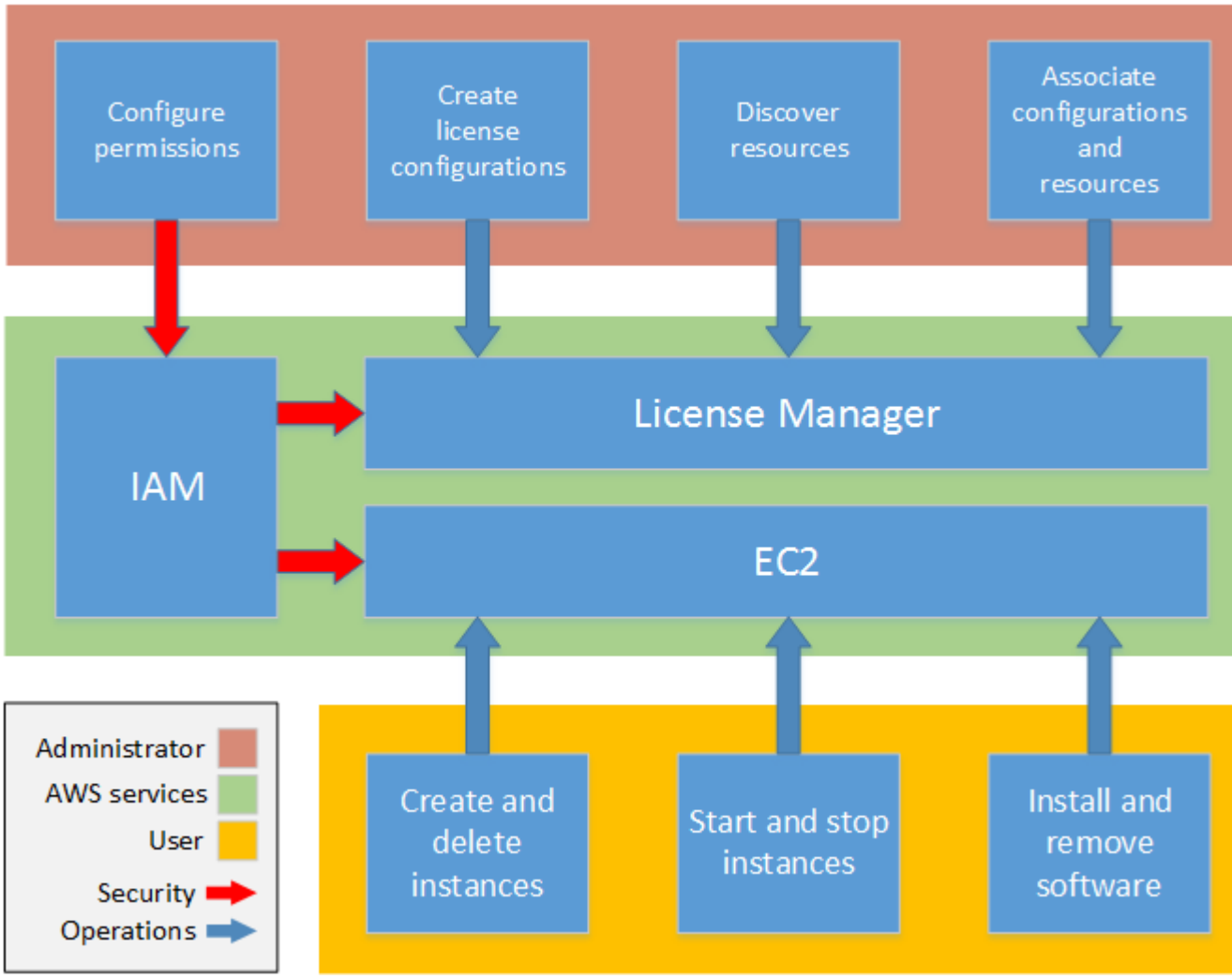
License Manager in the Enterprise

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 for the first time. Configure permissions for License Manager and its supporting services, and then configure permissions for your license administrator and the user accounts to consume managed licenses. To configure cross-account inventory search, see Configuring License Manager Settings (p. 11).

Using AWS License Manager

This section describes the license-related operations handled by AWS License Manager and shows how to perform them using the License Manager console. 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 service, 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.

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 master 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:

- US West (N. California)
- Canada (Central)
- EU (Paris)
- EU (Stockholm)
- South America (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Contents

Using License Configurations

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.

License Configuration Overview

A license configuration consists of basic parameters and of rules that vary according to the parameter values. For more information about the creation and structure of license configurations, see CreateLicenseConfiguration and the LicenseConfiguration type definition. Available parameters and rules include the following:

- **License counting type** — The metric used to count licenses. Supported values are physical core, vCPU, socket, and instance.

  (Optional) Rules following from counting type value:

  - **Core:** `minimumCores`, `maximumCores`
  - **vCPU:** `minimumVcpus`, `maximumVcpus`
  - **Socket:** `minimumSockets`, `maximumSockets`

  (Optional) Rules common to all counting types:

  - `honorVcpuOptimization` — License Manager integrates with CPU optimization support in Amazon EC2, which allows you to customize the number of vCPUs running on an instance. The `honorVcpuOptimization` rule determines how License Manager counts licenses when CPU optimization has been configured. If the rule is set to *True*, vCPUs are counted based on the customized core and thread count. If the rule is set to *False*, License Manager counts the default number of vCPUs for the instance type.
  - `allowedTenancy` — Allowed EC2 tenancy type for the AWS resource consuming a license. Options are:
    - Shared tenancy (default)
    - Dedicated Instance
    - Dedicated Host
- **(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.

In addition to rules, each configuration includes metadata fields, such as:

- **Name**
- **Description**
- **Number of licenses consumed**
- **Status** (controls whether the configuration is active)

You can also attach tags (consisting of customizable key-value pairs) to your license configurations.

After a license configuration has been created and attached to a running instance, the number of licenses and the usage limit can be modified by a License Manager administrator to reflect changing resource needs.

Building License Manager Rules from Vendor Licenses

This section explores how to create License Manager rule sets based on the language of software vendor licenses. The examples that follow are not intended as blueprints for actual customer 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 table below associates the License Manager rule-making parameters with the vendor licensing requirements that they capture and automate.

> **Important**
> The numbers in this example are for illustration purposes only. Do not use these numbers as a template for your own license configurations.

License Manager Rule	**Settings (*example values only*)**
License counting type	**Console option:** **License Type** is set to **Cores**.
License count	**Console option:** **Number of cores** is set to **96**.
Minimum / Maximum vCPUs or cores (optional)	**Console options:** **Minimum cores** is set to **8**.

License Manager Rule	Settings (*example values only*)
	Maximum cores is set to **16**.
License count hard limit (optional)	**Console option:** **Enforce license limit** is selected.
Allowed tenancy (optional)	**Console option:** **Tenancy** is set to **Dedicated Host**.

Creating, Modifying, and Deleting License Configurations in the Console

This section provides example procedures for creating and managing license configurations in the License Manager console.

To create 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. Choose **Create license configuration**.
4. In the **Configuration details** panel, provide the following information as needed:

   - **Name** — A name to identify the license configuration.
   - **Description** — A description of the license configuration.
   - **License type** — The counting metric for this license (vCPUs, Cores, Sockets, or Instances).
   - **Number of vCPUs** or **Number of Cores** — The option displayed depends on the counting metric. 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, a hard limit is imposed.
5. Expand the **Additional configuration** section and provide information for the following rules as needed. You can create and combine multiple rules.

   - **Minimum vCPUs**, **Minimum Cores**, or **Minimum Sockets** — The option displayed depends on the license counting metric. This value is an integer.
   - **Maximum vCPUs**, **Maximum cores**, or **Maximum Sockets** — The option displayed depends on the license counting metric. This value is an integer.
   - **Tenancy** — Available values are **Shared**, **Dedicated Host**, and **Dedicated Instance**. If no tenancy type is specified, all are accepted.

   Choose **Add rule** when done with each rule.
6. In the **Tags** pane, you can optionally apply tags to your license configuration. Tags are key-value pairs.

   Provide the following information:

   - **Key** — The searchable name of the key.
   - **Value** — The value for the key.

   Choose **Add tag**. You can create and add multiple tags.

7. Choose **Create**. The console returns you to the **License configurations** page, which lists and describes your existing license configurations.

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. Choose **Action**, **Edit**.
4. Edit the fields as needed and then choose **Save**.

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.

To deactivate a license configuration

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.

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 **Action**, **Deactivate**, **Deactivate**.

To delete 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. For **License configurations**, select the one to delete and choose **Details**.
4. For **Resources**, select each of the resources (individually or in bulk) and choose **Disassociate**. Repeat until the list is empty.
5. Choose **Action**, **Delete**, **Delete**.

Creating, Modifying, and Deleting License Configurations with the License ManagerAPI, AWS CLI, and SDKs

For information about the License Manager API, AWS CLI, and SDKs, see the following documentation:

- AWS License Manager API Reference
- License Manager section of the AWS CLI Command Reference
- Tools for Amazon Web Services: SDKs

Enforcing License Rules

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.

> **Note**
> 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.

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 Amazon EC2 Systems Manager Automation, AWS 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.

Manually Associating License Configurations with AMIs

The following procedure demonstrates how to associate and disassociate license configurations from AMIs using the License Manager console. The procedures assume that you have at least one existing license configuration already configured. You can associate license configurations with any AMI that you have access to, whether owned or shared.

To associate a license configuration with 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. For **License configurations**, choose the license configuration with which to work.

4. Choose **Actions**, **Associate AMI**. The **Associated Amazon Machine Images** list displays the AMIs already associated with the license configuration (if any).
5. Choose **Associate a new AMI**.
6. For **Available AMIs**, select one or more AMIs and choose **Associate AMI**, **OK**. Any new AMIs that you associated now appear in the **Associated Amazon Machine Images** list.

To disassociate a license configuration from 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. For **License configurations**, select the license configuration with which to work.
4. Choose **Associated AMIs**.
5. For **Associated Amazon Machine Images**, select the AMI to disassociate and choose **Disassociate AMI**, **Disassociate**.

Discovering Resource Inventory with License Manager

License Manager allows you to discover on-premises applications using Systems Manager (SSM) 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.

SSM 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. Once inventory data has been purged from SSM, License Manager marks the instance as inactive and updates local inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in SSM so that License Manager can run cleanup operations.

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.

Setting Up and Using Inventory Search

Complete the following steps to search your resource inventory.

1. Configure Systems Manager (SSM) Inventory on every host to manage. This includes on-premises and other non-AWS resources.
2. Create license configurations for the servers and applications to discover.
3. To use cross-account inventory discovery by integrating License Manager with your AWS Organizations account, enable this feature in Configuring License Manager Settings (p. 11).
4. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
5. Choose **Search inventory** section of the License Manager console and confirm whether cross-account inventory discovery is enabled.

6. To perform a filtered search for available resources, enter a filter term such as an application name, a platform name, or a resource ID in the search box. You can also apply logical operators to your search terms. Press Enter.

Associating License Configurations with Discovered Inventory

After you have identified your unmanaged resources, manage them by associating license configurations.

To associate a license configuration with a resource

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Search inventory**.
3. Filter the **Search inventory** list by entering a filter term such as an application name, a platform name, or a resource ID. You can also apply logical operators to your search terms. Press Enter.
4. Select the inventory items to associate with a license configuration and choose **Associate license configuration**.
5. (Optional) Select **Share license configuration with all my member accounts**.
6. Choose the appropriate license configuration and choose **Associate**.

To disassociate a license configuration from 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 with which to work.
4. Choose **Associated resources**.
5. Select each of the resources to disassociate from the license configuration and choose **Disassociate resource**.

Configuring License Manager Settings

The **Settings** section of the License Manager console display settings for the logged-in account in License Manager and allows you to edit those settings. Settings displayed in the **Account settings** panel include:

- **Account type**
- **S3 Bucket**
- **Link AWS Organizations account**
- **Cross-account resource discovery**
- **SNS Topic ARN**

Each field contains a value or status for the setting.

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**, **Edit**.
3. In the **Account management** panel, review and edit the following settings as needed.

Important
To enable cross-account inventory discovery, you must configure the items in this panel, linking your AWS Organizations account with License Manager, and applying permissions for cross-account inventory search.

- **Link AWS Organizations accounts**

  You can configure a single master account (your AWS Organizations account) to perform license configuration attachments on instances in child accounts.

  Select this field to associate your AWS Organizations account with your License Manager account. License Manager performs this action automatically.

  To enable this option, you must be signed into your master account and have all features enabled in AWS Organizations. For more information, see Enabling All Features in Your Organization.

  Linking your AWS Organizations account also creates an AWS Resource Access Manager resource share in your master account and associates your account with it. This allows you to seamlessly share license configurations. For more information, see What Is AWS RAM?.

- **Cross-account inventory search**

  License Manager uses Amazon EC2 Systems Manager (SSM) inventory to discover software usage. Querying SSM inventory requires SSM Resource Data Sync to store inventory in an Amazon S3 bucket, Amazon Athena to aggregate SSM inventory data from organizational accounts, and AWS Glue to provide a fast query experience. Ensure that you have configured SSM inventory on all of your resources.

  Select this field to configure permissions for the associated services and locations that License Manager uses perform cross-account inventory search. License Manager performs these actions automatically.

4. Under **Simple Notification Service (SNS)**, you can modify the Amazon SNS topic ARN.
5. Choose **Save**.

Using the License Manager Dashboard

The **Dashboard** section of the 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

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.

For information about other services that support service-linked roles, see AWS Services That Work with IAM. Look for the services that have **Yes** in the **Service-Linked Role** column. To view the service-linked role documentation for that service, choose a **Yes** with a link.

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

Contents

Using the Core License Manager Role

This topic describes the License Manager role, a service-linked role that License Manager requires for its core functions.

Permissions for the Core License Manager Role

License Manager uses the service-linked role named `AWSServiceRoleForAWSLicenseManagerRole`. This allows License Manager access to AWS resources to manage licenses on your behalf.

The `AWSServiceRoleForAWSLicenseManagerRole` service-linked role trusts the following service to assume the role:

- `license-manager.amazonaws.com`

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

- Action: `s3:GetBucketLocation` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:ListBucket` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:PutObject` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `sns:Publish` on `arn:aws:sns:*:*:aws-license-manager-service-*`
- Action: `sns:ListTopics` on `*`
- Action: `ec2:DescribeInstances` on `*`
- Action: `ec2:DescribeImages` on `*`
- Action: `ec2:DescribeHosts` on `*`
- Action: `ssm:ListInventoryEntries` on `*`
- Action: `ssm:GetInventory` on `*`
- Action: `ssm:CreateAssociation` on `*`
- Action: `organizations:ListAWSServiceAccessForOrganization` on `*`
- Action: `organizations:DescribeOrganizationon *`

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "S3BucketPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::aws-license-manager-service-*"
            ]
        },
        {
            "Sid": "S3ObjectPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-license-manager-service-*"
            ]
        },
        {
            "Sid": "SNSAccountPermissions",
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-license-manager-service-*"
            ]
        },
        {
            "Sid": "SNSTopicPermissions",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": [
                "*"
            ]
        },
```

```
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeHosts"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:ListInventoryEntries",
                "ssm:GetInventory",
                "ssm:CreateAssociation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a Service-Linked Role for 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.

Creating a Service-Linked Role in License Manager

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. 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.

Editing 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*.

Deleting 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.

Cleaning 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 operation again.

To delete License Manager resources used by the AWSServiceRoleForAWSLicenseManagerRole

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 steps 2 and 3 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. 17) and

AWSLicenseManagerMemberAccountRole (p. 23), delete those roles first. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for License Manager Service-Linked Roles

License Manager supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

Region name	Region identity	Support in License Manager
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka-Local)	ap-northeast-3	No
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	No
EU (Frankfurt)	eu-central-1	Yes
EU (Ireland)	eu-west-1	Yes
EU (London)	eu-west-2	Yes
EU (Paris)	eu-west-3	No
South America (São Paulo)	sa-east-1	No
AWS GovCloud (US)	us-gov-west-1	No

Using the License Manager–Master Account Role

This topic describes License Manager–Master Account, the service-linked role that License Manager requires to perform centralized, cross-account, license management.

Permissions for License Manager–Master Account Role

License Manager–Master Account uses the service-linked role named `AWSServiceRoleForAWSLicenseManagerMasterAccountRole`. The role allows License Manager

access to AWS resources to manage license management operations for a central master account on your behalf.

The `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` service-linked role trusts the following service to assume the roles:

- `license-manager.master-account.amazonaws.com`

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

- Action: `s3:GetBucketLocation` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:ListBucket` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:GetLifecycleConfiguration` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:PutLifecycleConfiguration` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:GetBucketPolicy` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:PutBucketPolicy` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:AbortMultipartUpload` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:PutObject` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:GetObject` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:ListBucketMultipartUploads` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:ListMultipartUploadParts` on `arn:aws:s3:::aws-license-manager-service-*`
- Action: `s3:DeleteObject` on `arn:aws:s3:::aws-license-manager-service-*/resource_sync/*`
- Action: `athena:GetQueryExecution` on `*`
- Action: `athena:GetQueryResults` on `*`
- Action: `athena:StartQueryExecution` on `*`
- Action: `glue:GetTable` on `*`
- Action: `glue:GetPartition` on `*`
- Action: `glue:GetPartitions` on `*`
- Action: `organizations:DescribeOrganization` on `*`
- Action: `organizations:ListAccounts` on `*`
- Action: `organizations:DescribeAccount` on `*`
- Action: `organizations:ListChildren` on `*`
- Action: `organizations:ListParents` on `*`
- Action: `organizations:ListAccountsForParent` on `*`
- Action: `organizations:ListRoots` on `*`
- Action: `organizations:ListAWSServiceAccessForOrganization` on `*`
- Action: `ram:GetResourceShares` on `*`
- Action: `ram:GetResourceShareAssociations` on `*`
- Action: `ram:TagResource` on `*`
- Action: `ram:CreateResourceShare` on `*`
- Action: `ram:AssociateResourceShare` on `*`

- Action: `ram:DisassociateResourceShare` on `*`
- Action: `ram:UpdateResourceShare` on `*`
- Action: `ram:DeleteResourceShare` on `*`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "S3BucketPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-license-manager-service-*"
            ]
        },
        {
            "Sid": "S3ObjectPermissions1",
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::aws-license-manager-service-*"
            ]
        },
        {
            "Sid": "S3ObjectPermissions2",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
            ]
        },
        {
            "Sid": "AthenaPermissions",
            "Effect": "Allow",
            "Action": [
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StartQueryExecution"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
            "Sid": "GluePermissions",
            "Effect": "Allow",
            "Action": [
                "glue:GetTable",
                "glue:GetPartition",
                "glue:GetPartitions"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListAccountsForParent",
                "organizations:ListRoots",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "RAMPermissions1",
            "Effect": "Allow",
            "Action": [
                "ram:GetResourceShares",
                "ram:GetResourceShareAssociations",
                "ram:TagResource"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "RAMPermissions2",
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Service": "LicenseManager"
                }
            }
        },
        {
            "Sid": "RAMPermissions3",
            "Effect": "Allow",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "ram:ResourceTag/Service": "LicenseManager"
                }
            }
        }
    ]
}
```

Creating a License Manager–Master 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 the AWSServiceRoleForAWSLicenseManagerMasterAccountRole role in your account. For more information, see A New Role Appeared in My IAM Account.

Creating a License Manager–Master Account Service-Linked Role

You can use the License Manager console to create this 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 **Settings**, **Edit**.
3. Choose **Link AWS Organization accounts**.
4. Choose **Apply**.

You can also use the IAM console to create a service-linked role with the **License Manager**–Master Account use case. 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.

Editing 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*.

Deleting a Service-Linked Role for License Manager

You don't need to manually delete the AWSServiceRoleForAWSLicenseManagerMasterAccountRole role. When you CompleteThisDeleteActionInThisService-2 in the AWS Management Console, the AWS CLI, or the AWS API, License Manager cleans up the resources and deletes the service-linked role for you.

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*.

Supported Regions for License Manager Service-Linked Roles

License Manager supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

License Manager does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForAWSLicenseManagerMasterAccountRole role in the following Regions.

Region name	Region identity	Support in License Manager
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka-Local)	ap-northeast-3	No
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	No
EU (Frankfurt)	eu-central-1	Yes

Region name	Region identity	Support in License Manager
EU (Ireland)	eu-west-1	Yes
EU (London)	eu-west-2	Yes
EU (Paris)	eu-west-3	No
South America (São Paulo)	sa-east-1	No
AWS GovCloud (US)	us-gov-west-1	No

Using the License Manager–Member Account Role

This topic describes License Manager–Member Account, the service-linked role that License Manager requires to allow the master account to manage licenses.

Permissions for License Manager–Member Account Role

License Manager–Member Account uses the service-linked role named `AWSServiceRoleForAWSLicenseManagerMemberAccountRole`. This role allows License Manager to access AWS resources for license management operations from a configured master account on your behalf.

The `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` service-linked role trusts the following services to assume the role:

- `license-manager.member-account.amazonaws.com`

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

- Action: `license-manager:UpdateLicenseSpecificationsForResource` on `*`
- Action: `ssm:ListInventoryEntries` on `*`
- Action: `ssm:GetInventory` on `*`
- Action: `ssm:CreateAssociation` on `*`
- Action: `ssm:CreateResourceDataSync` on `*`
- Action: `ssm:DeleteResourceDataSync` on `*`
- Action: `ssm:ListResourceDataSync` on `*`
- Action: `ssm:ListAssociations` on `*`
- Action: `ram:AcceptResourceShareInvitation` on `*`
- Action: `ram:GetResourceShareInvitations` on `*`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

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

```
    "Statement": [
        {
            "Sid": "LicenseManagerPermissions",
            "Effect": "Allow",
            "Action": [
                "license-manager:UpdateLicenseSpecificationsForResource"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:ListInventoryEntries",
                "ssm:GetInventory",
                "ssm:CreateAssociation",
                "ssm:CreateResourceDataSync",
                "ssm:DeleteResourceDataSync",
                "ssm:ListResourceDataSync",
                "ssm:ListAssociations"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "RAMPermissions",
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Creating a Service-Linked Role for License Manager–Member Account

You don't need to manually create a service-linked role. When you enable integration with AWS Organizations from the master account in the License Manager console on the **Settings** page, the AWS CLI using `update-service-settings`, or the AWS API using `UpdateServiceSettings`, 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 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 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.

Creating a Service-Linked Role in License Manager

You can use License Manager commands from the AWS Command Line Interface to create a service-linked role.

To create a service-linked role

1. Log into your AWS Organizations master 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 Organization accounts**.
5. Choose **Apply**. This creates the roles AWSServiceRoleForAWSLicenseManagerRole (p. 13) and AWSServiceRoleForAWSLicenseManagerMemberAccountRole (p. 23) 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. 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.

Editing 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*.

Deleting a Service-Linked Role for License Manager

You don't need to manually delete the AWSServiceRoleForAWSLicenseManagerMemberAccountRole role. When you CompleteThisDeleteActionInThisService-3 in the AWS Management Console, AWS CLI, or AWS API, License Manager cleans up the resources and deletes the service-linked role for you.

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*.

Supported Regions for License Manager Service-Linked Roles

License Manager supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

License Manager does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForAWSLicenseManagerMemberAccountRole role in the following Regions.

Region name	Region identity	Support in License Manager
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka-Local)	ap-northeast-3	No
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	No
EU (Frankfurt)	eu-central-1	Yes
EU (Ireland)	eu-west-1	Yes
EU (London)	eu-west-2	Yes
EU (Paris)	eu-west-3	No
South America (São Paulo)	sa-east-1	No
AWS GovCloud (US)	us-gov-west-1	No

Logging AWS License Manager API Calls with 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 AWS 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"
}
```

Troubleshooting AWS License Manager

This section contains troubleshooting help for specific errors that you may encounter when using AWS License Manager. Before using these procedures, confirm that your License Manager setup meets the requirements stated in Configuring License Manager Settings.

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 master 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 master account pool. To allow the master account to disassociate resources, restore the SLR.

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

Systems Manager Inventory Is Out of Date

SSM 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. Once inventory data has been purged from SSM, License Manager marks the instance as inactive and updates local inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in SSM so that License Manager can run cleanup operations.

Apparent Persistence of 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 Slow to Appear in Master 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 master 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 master account.

After Enabling Cross-Account Mode, Child Account Instances 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

Once 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 master 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 master account.

Document History for AWS License Manager

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

- **API version: latest**
- **Latest documentation update:** November 28, 2018

Change	Description	Date
AWS License Manager initial release	Initial documentation for service launch	November 28, 2018

AWS Glossary

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