aws

User Guide

AWS License Manager

AWS License Manager: User Guide

Table of Contents

What is AWS License Manager? 1
Managed entitlements 1
License Manager use cases 2
Related services 3
How License Manager works 5
Get started 8
Working with License Manager 9
Self-managed licenses 10
Parameters and rules 11
Build rules from vendor licenses 13
Create a self-managed license 14
Share a self-managed license 16
Edit a self-managed license 21
Deactivate a self-managed license 21
Delete a self-managed license 22
License rules 22
Associating self-managed licenses and AMIs 24
Disassociating self-managed licenses and AMIs 25
Usage reports 25
Create a usage report 26
Edit a usage report 27
Delete a usage report 27
License type conversions 28
Eligible license types 29
Prerequisites 38
Convert a license type 41
Tenancy conversion 50
Troubleshooting 52
Host resource groups 54
Create a host resource group 55
Share a host resource group 56
Add Dedicated Hosts to a host resource group 56
Launch an instance in a host resource group 57
Modify a host resource group 57

Remove Dedicated Hosts from a host resource group ... 57
Delete a host resource group ... 58
Inventory search ... 58
Work with inventory search ... 59
Automated discovery of inventory ... 65
Granted licenses ... 67
View your granted licenses ... 68
Manage your granted licenses ... 68
Distribute entitlements ... 72
Grant acceptance and activation ... 73
License status ... 76
Metrics for buyer accounts ... 77
Seller issued licenses ... 78
Entitlements ... 79
License usage ... 79
Required permissions ... 80
Create seller issued licenses ... 82
Grant seller issued licenses ... 83
Temporary credentials for ISV customers ... 84
Check out seller issued licenses ... 85
Delete seller issued licenses ... 86
User-based subscriptions ... 86
Considerations ... 87
Subscription charges in License Manager ... 88
User-based subscription prerequisites ... 93
Supported software subscriptions ... 102
Active Directory ... 103
Additional software ... 104
Get started ... 104
Configure GPO for more sessions ... 114
Launch an instance from a license included AMI ... 115
Connect to an instance ... 116
Modify firewall settings for Microsoft Office ... 117
Manage subscription users ... 118
Deregister Active Directory ... 119
Troubleshoot ... 120

Manage Linux subscriptions ... 123
Configure discovery ... 125
View instance data ... 131
Billing information ... 133
Manage CloudWatch alarms ... 135
Settings ... 138
Edit License Manager settings ... 139
Managed license settings ... 139
Linux subscription settings ... 141
User-based subscription settings ... 144
Delegated administrator settings ... 145
Dashboard ... 150
Monitoring License Manager ... 152
Monitoring with CloudWatch ... 152
Creating CloudWatch alarms ... 154
CloudTrail logs ... 154
License Manager information in CloudTrail ... 155
Understanding License Manager log file entries ... 156
Security ... 157
Data protection ... 158
Encryption at rest ... 159
Identity and access management ... 159
Create users, groups, and roles ... 159
IAM policy structure ... 160
Create IAM policies for License Manager ... 160
Grant permissions to users, groups, and roles ... 162
Service-linked roles ... 163
Core role ... 163
Management account role ... 166
Member account role ... 168
User-based subscription role ... 170
Linux subscriptions role ... 171
AWS managed policies ... 173
AWSLicenseManagerServiceRolePolicy ... 174
AWSLicenseManagerMasterAccountRolePolicy ... 176
AWSLicenseManagerMemberAccountRolePolicy ... 180

AWSLicenseManagerConsumptionPolicy 181
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 181
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 183
Policy updates 185
License signing 188
Compliance validation 190
Resilience 191
Infrastructure security 191
VPC endpoints with AWS PrivateLink 192
Create an interface VPC endpoint for License Manager 192
Create a VPC endpoint policy for License Manager 192
Troubleshooting 194
Cross-account discovery error 194
Management account cannot disassociate resources from a self-managed license 194
Systems Manager Inventory is out of date 194
Apparent persistence of a de-registered AMI 195
New child account instances are slow to appear in resource inventory 195
After enabling cross-account mode, child account instances are slow to appear 195
Cross-account discovery cannot be disabled 195
Child account user cannot associate shared self-managed license with an instance 195
Linking AWS Organizations accounts fails 196
User subscription product configuration failing 196
User subscription instances failing to launch 197
Seamless domain join for EC2 instances with user subscription products doesn't work 197
Unable to delete active directory 197
VPC endpoint was created in my account 198
Remove all VPC endpoint resources created by License Manager 198
Unable to delete AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service Linked Role (SLR) 198
Subscription is not present error for RDS SAL product 198
Troubleshooting trusts 199
Billing issues for user subscriptions 199
User subscription products show Marketplace subscription status of Inactive 200
Change a username on Managed Active Directory 200
Dissociate users from a terminated instance 200
User limits per instance 201

Installing additional software on user subscription instances 201
Japanese Language Packs on user subscription instances 201
Local Administrator user on user subscription instances 201
Unhealthy instances 202
Number of users that can RDP to a user subscriptions instance 202
Supported Windows operating systems 202
Supported versions of Office and Visual Studio 202
Using user subscription with older Windows Server versions 202
Using License Manager user subscriptions across accounts or regions 203
CAL token handling during migration to RDS SAL 203
Users in my self-managed AD with User subscription products 203
Tips for contacting AWS Support 204
Document history 205

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 model (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.

License Manager use cases

The following are examples of the functionality provided by License Manager for various use cases:

- Self-managed licenses in License Manager – Used to define licensing rules based on the terms of your enterprise agreements which determine how AWS processes commands that consume these licenses.
- Seller issued licenses in License Manager – Used to manage and distribute software licenses to end-users.
- Granted licenses in License Manager – Used to govern the use of licenses acquired from the AWS Marketplace, AWS Data Exchange, or directly from a seller who integrated their software with managed entitlements.

- License type conversions in License Manager – Used to change your license type between AWS provided licensing and the Bring Your Own License model (BYOL) without redeploying your workloads.
- Inventory search in License Manager – Used to discover and track on-premises applications using AWS Systems Manager Inventory and licensing rules.
- Use License Manager user-based subscriptions for supported software products – Used to purchase fully compliant Amazon provided licenses for supported software with a per user subscription fee.
- Manage Linux subscriptions in License Manager – Used to view and manage commercial Linux subscriptions you own and run on AWS.

Related services

License Manager is integrated with Amazon EC2, Amazon RDS, AWS Marketplace, AWS Systems Manager, and AWS Organizations.

The Amazon EC2 integration allows you to track licenses for the following resources and enforce licensing rules throughout the resource lifecycle:

- Amazon EC2 instances
- Dedicated Instances
- Dedicated Hosts
- Spot Instances and Spot Fleet
- Managed nodes

When you use 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 with AWS Organizations to manage all of your organizational accounts centrally.

Additionally, you can govern the use of licenses purchased from AWS Marketplace, AWS Data Exchange, or directly from a seller who integrated their software with AWS License Manager. You can use AWS License Manager to distribute rights of use, known as entitlements, to specific AWS accounts.

License Manager integrates with Amazon RDS for Oracle and Amazon RDS for Db2 vCPU-based BYOL licenses. With this integration, you gain visibility into vCPU usage for your RDS for

Oracle and RDS for Db2 DB instances. You can use this data to calculate the number of licenses consumed based on your licensing terms with the database management system vendors. For more information, see the following associated links in the *Amazon RDS User Guide*.

- RDS for Oracle licensing options
- RDS for Db2 licensing options

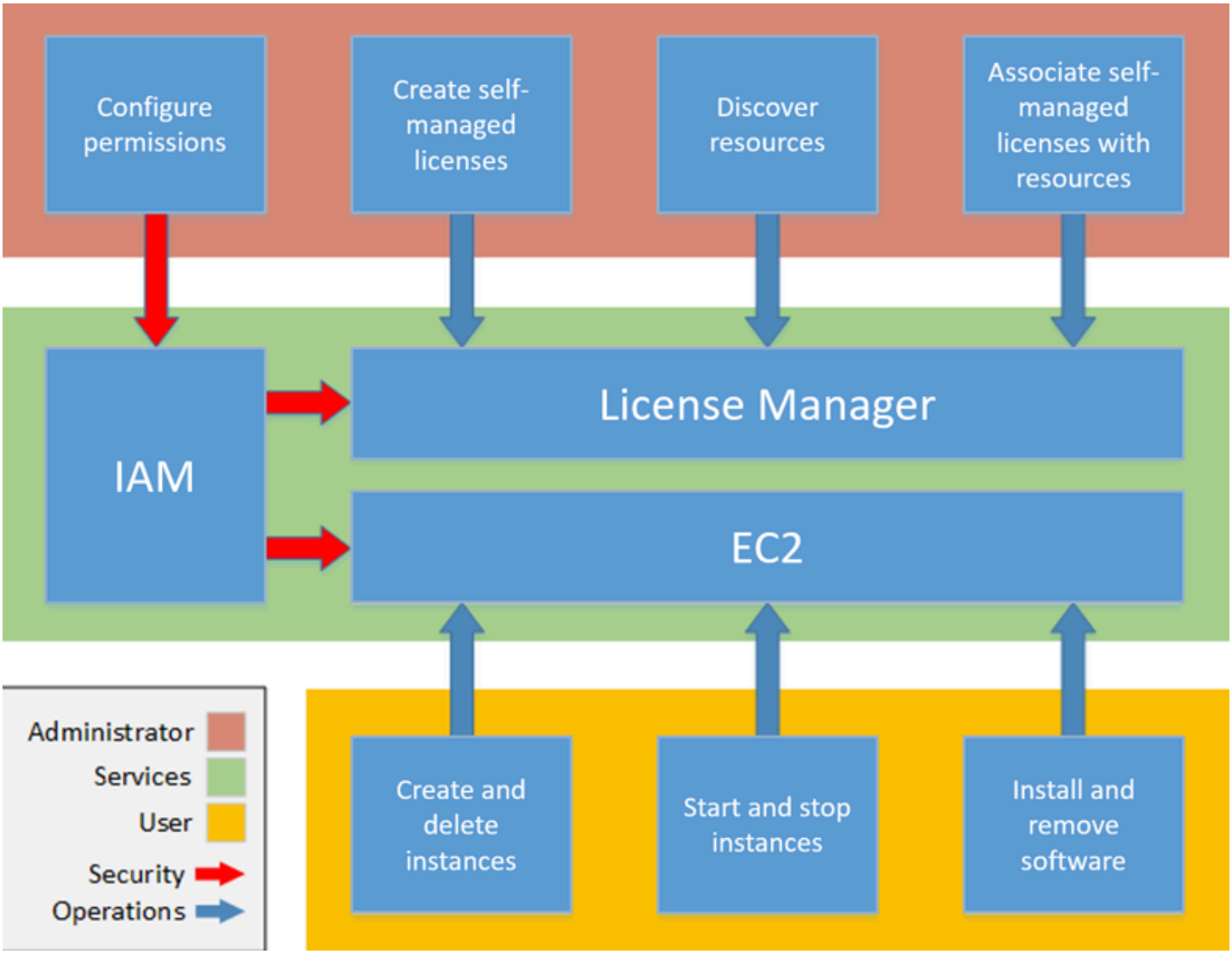
How License Manager works

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 self-managed licenses, taking inventory of computing resources both on-premises and in the cloud, and associating self-managed licenses with discovered resources. In practice, this could mean associating a self-managed license 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.

Get started with License Manager

To use AWS License Manager, you must first complete onboarding steps. The following procedure walks you through the onboarding steps in the AWS Management Console.

Get started with License Manager

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. You are prompted to configure permissions for License Manager and its supporting services. Follow the directions to configure the required permissions.
3. With the initial setup complete, you can proceed with using License Manager for your desired License Manager use cases.

For more information on managing permissions for users, groups, and roles to utilize License Manager while following AWS best practices, see Identity and access management for License Manager. For more information about setting up your Amazon EC2 resources that integrate with License Manager, see Set up to use Amazon EC2 in the *Amazon Elastic Compute Cloud User Guide*.

Working with 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 self-managed licenses, take inventory of your license-consuming resources, associate self-managed 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 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.

Contents

- Self-managed licenses in License Manager
- License rules in License Manager
- Usage reports in License Manager
- License type conversions in License Manager
- Host resource groups in License Manager
- Inventory search in License Manager
- Granted licenses in License Manager
- Seller issued licenses in License Manager
- Use License Manager user-based subscriptions for supported software products
- Manage Linux subscriptions in License Manager
- Settings in License Manager
- Dashboard in License Manager

Self-managed licenses in License Manager

Self-managed licenses (formerly known as *license configurations*) are the core of License Manager. Self-managed licenses 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 self-managed licenses, work closely with your organization's compliance team to review your enterprise agreements.

AWS services such as License Manager have service quotas that define the maximum number of resources or operations per Region that are available to your AWS account for that service. For example, with License Manager, you can have a maximum of 10 self-managed licenses per resource, with no more than 25 self-managed licenses total in any given AWS Region. To find out more about License Manager quotas, see AWS License Manager Service quotas in the *AWS General Reference*.

> **Note**
>
> Systems Manager managed instances must be associated with vCPU and instance type self-managed licenses.

Contents

- Self-managed license parameters and rules in License Manager
- Build License Manager rules from vendor licenses
- Create a self-managed license in License Manager
- Share a self-managed license in License Manager
- Edit a self-managed license in License Manager
- Deactivate a self-managed license in License Manager
- Delete a self-managed license in License Manager

Self-managed license parameters and rules in License Manager

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

Available parameters and rules include the following:

- **Self-managed license name** – The name of the self-managed license.
- **(Optional) Description** – A description of the self-managed license.
- **License type** – The metric used to count licenses. Supported values are **vCPUs**, **Cores**, **Sockets**, and **Instances**.
- **(Optional) Number of <option>** – 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. The supported products are Windows Server, SQL Server, Amazon RDS for Oracle, and Amazon RDS for Db2.
- **(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`	✓	✓	✓	✓

Console name	API name	Cores	Instances	Sockets	vCPUs
vCPU Optimization	`honorVcpu Optimization`				✓

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 self-managed licenses.

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 self-managed license in License Manager

A self-managed license represents the licensing terms in the agreement with your software vendor. Your self-managed license 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.

Considerations for Amazon RDS for Oracle and Amazon RDS for Db2 databases

When you add product information to configure automated discovery of Amazon RDS for Oracle or Amazon RDS for Db2 databases, 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 self-managed license.
- You cannot track Amazon RDS databases and other products using the same self-managed license.

To create a self-managed license using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **self-managed licenses**.
3. Choose **Create self-managed license**.
4. In the **Configuration details** panel, provide the following information:
   - **Self-managed license name** – A name for the self-managed license.
   - **Description** – An optional description of the self-managed license.
   - **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.

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 self-managed license. 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 self-managed license using the command line

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

Share a self-managed license in License Manager

You can use AWS Resource Access Manager to share your self-managed licenses with any AWS account or through AWS Organizations. For more information, see Sharing your AWS resources in the *AWS RAM User Guide*.

Share a self-managed license with your AWS Organization

Prerequisites

To complete this procedure, you must link your AWS Organization with License Manager. For more information, see Managed license settings in License Manager.

Share your license

To share a self-managed license with your AWS Organization, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.

3. Select the self-managed license.
4. Choose **Share with AWS organization accounts** from the **Actions** menu.

Supported accounts quota

If you enabled license sharing in AWS License Manager before October 14, 2023, your quota for the maximum number of accounts that License Manager supports within your organization will be less than the new default maximum. You can increase this quota by using API operations for AWS RAM that are provided in the following section. For more information about the default quotas in License Manager, see Quotas for working with licenses in the *AWS General Reference guide*.

Prerequisites

To complete the following procedure, you must sign in as a principal in the organization's management account that has the following permissions:

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Increasing the supported accounts quota

The following procedure will increase your current quota for `Number of accounts per organization for License Manager` to the current default maximum.

To increase the supported accounts quota for License Manager

1. Use the describe-organization AWS CLI command to determine your organization's ARN by using the operation:

```
aws organizations describe-organization

{
 "Organization": {
  "Id": "o-abcde12345",
  "Arn": "arn:aws:organizations::111122223333:organization/o-abcde12345",
  "FeatureSet": "ALL",
```

```
  "MasterAccountArn": "arn:aws:organizations::111122223333:account/o-
abcde12345/111122223333",
  "MasterAccountId": "111122223333",
  "MasterAccountEmail": "name+orgsidentifier@example.com",
  "AvailablePolicyTypes": [
    {
     "Type": "SERVICE_CONTROL_POLICY",
     "Status": "ENABLED"
    }
  ]
 }
}
```

2. Use the get-resource-shares AWS CLI command to determine your organization's ARN by using the operation:

```
aws ram  get-resource-shares --resource-owner SELF --tag-filters
 tagKey=Service,tagValues=LicenseManager --region us-east-1

{
 "resourceShares": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "name": "licenseManagerResourceShare-111122223333",
    "owningAccountId": "111122223333",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "tags": [
     {
      "key": "Service",
      "value": "LicenseManager"
     }
    ],
    "creationTime": "2023-10-04T12:52:10.021000-07:00",
    "lastUpdatedTime": "2023-10-04T12:52:10.021000-07:00",
    "featureSet": "STANDARD"
  }
 ]
}
```

3. Use the enable-sharing-with-aws-organization AWS CLI command to enable resource sharing with AWS RAM:

```
aws ram enable-sharing-with-aws-organization

{
 "returnValue": true
}
```

You can use the list-aws-service-access-for-organization AWS CLI command to verify that Organizations lists service principals are enabled for License Manager and AWS RAM:

```
aws organizations list-aws-service-access-for-organization

{
 "EnabledServicePrincipals": [
  {
    "ServicePrincipal": "license-manager.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.814000-07:00"
  },
  {
    "ServicePrincipal": "license-manager.member-account.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.565000-07:00"
  },
  {
    "ServicePrincipal": "ram.amazonaws.com",
    "DateEnabled": "2023-10-04T13:06:34.771000-07:00"
  }
 ]
}
```

Important

It can take up to six hours for AWS RAM to finish this operation for your organization. This process must complete before you can proceed.

4. Use the associate-resource-share AWS CLI command to associate your License Manager resources share with your organization:

```
aws ram associate-resource-share --resource-share-arn arn:aws:ram:us-
east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --
principals arn:aws:organizations::111122223333:organization/o-abcde12345 --
region us-east-1
```

```
{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATING",
    "external": false
  }
 ]
}
```

You can use the get-resource-share-associations AWS CLI command to validate that the resource share association's `status` is ASSOCIATED:

```
aws ram get-resource-share-associations --association-type "PRINCIPAL" --principal
 arn:aws:organizations::111122223333:organization/o-abcde12345--resource-share-
arns arn:aws:ram:us-east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "resourceShareName": "licenseManagerResourceShare-111122223333",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATED",
    "creationTime": "2023-10-04T13:12:33.422000-07:00",
    "lastUpdatedTime": "2023-10-04T13:12:34.663000-07:00",
    "external": false
  }
 ]
}
```

Edit a self-managed license in License Manager

You can edit values for the following fields in a self-managed license:

- Self-managed license name
- Description
- Number of <option>
- Enforce license type limit

To edit a self-managed license

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

To edit a self-managed license using the command line

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

Deactivate a self-managed license in License Manager

When you deactivate a self-managed license, 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 self-managed license is deactivated, it must not be attached to any running instance. After deactivation, launches cannot be performed with the self-managed license.

To deactivate a self-managed license

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **self-managed licenses**.

3. Select the self-managed license.
4. Choose **Actions**, **Deactivate**. When prompted for confirmation, choose **Deactivate**.

To deactivate a self-managed license using the command line

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

Delete a self-managed license in License Manager

Before you can delete a self-managed license, you must disassociate any resources. You can delete a self-managed license 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 self-managed license, create a new self-managed license to reflect the updated terms and associate it with the existing resources.

To delete a self-managed license using the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license 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 self-managed license using the command line

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

License rules in License Manager

After self-managed license 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 self-managed licenses 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 self-managed license IDs in the **self-managed licenses** 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 self-managed licenses and AMIs

The following procedure demonstrates how to associate self-managed licenses with AMIs using the License Manager console. The procedure assumes that you have at least one existing self-managed license. You can associate self-managed licenses 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 self-managed license in the current account. Otherwise, you can specify whether the AMI is associated with the self-managed license across all accounts or only in the current account.

If you associate an AMI with a self-managed license 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.

If you copy an AMI within the same Region, and that AMI has associated license configurations, those license configurations are automatically associated with the new AMI. When you launch an instance from the new AMI, License Manager tracks it. Similarly, if you create a new AMI from a running instance that has associated license configurations, those license configurations are automatically associated with the new AMI, and License Manager tracks the instances that you launch from the new AMI.

> **Warning**
>
> License Manager does not support cross-Region instance tracking. If you copy an AMI that has associated license configurations to a different Region, License Manager blocks all instance launches from the new AMI.

To associate a self-managed license and an AMI

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license 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 self-managed licenses and AMIs

The following procedure demonstrates how to disassociate self-managed licenses 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 self-managed license and an AMI

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

Usage reports in License Manager

Using AWS License Manager you can track the history of your self-managed licenses by scheduling periodic snap shots of your license usage. By setting up usage reports License Manager will automatically upload reports of your self-managed licenses to an S3 bucket based on your specifications. Usage reports were formerly called report generators. You can set up multiple usage reports 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 usage report, reports are no longer published to your S3 bucket.

Create a usage report in License Manager

When you create a usage report you specify a self-managed license 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 usage report can produce one or more of following report types.

Self-managed license summary report

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

Resource usage report

This report type gives you details about your tracked resources and their license consumption. Each tracked resource using the specified self-managed license 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 usage report

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. From the navigation panel choose **Usage reports**.
3. Choose **Create usage report**, then from the **Create usage report** pane define the parameters for the report:
   a. Enter a **Name** and optional **Description** for your usage report.
   b. Select a self-managed license type from the drop down list. This is the type of license that the usage report 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 24 hours**, **Once every 7 days** or **Once every 30 days**.
   e. (Optional) Add **Tags** to track the usage report resource.
4. Select **Create usage report**.

A new usage report 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 usage report. 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 S3 URI pattern:

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

Edit a usage report in License Manager

You can view and make changes to your usage reports from the License Manager console at any time. The **usage reports** table lists all the usage reports 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 usage reports, and view the status of report generation.

To edit a usage report

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

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

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

Delete a usage report in License Manager

Deleting a usage report 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 self-managed license from your account if it has a usage report associated. You must first delete that usage report.

To edit a usage report

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

License type conversions in License Manager

With License Manager, you can change your license type between AWS provided licensing and Bring Your Own License model (BYOL) as your business needs change. You can change your license type 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 Elastic Compute Cloud (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. You can change to BYOL so that you can use the licenses that were released during the migration.

Continue running workloads with expiring license agreements

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. You might choose to do this if your license agreement with the operating system's software vendor, such as Microsoft or Canonical, is about to expire and you do not plan to renew it.

Optimize costs

For small or irregular workloads, AWS provided licenses (license included) instances might be more cost effective. When you choose to use BYOL these options might require a longer term

commitment. For this case, you can use License Manager license type conversion to switch your instances to license included to optimize licensing related costs. If your instances were launched from your own virtual machine (VM) image, you can switch back to BYOL. You might choose to do this when the workload is more steady or predictable.

Extended maintenance

If your Ubuntu operating system has reached the end of standard support, you can add a paid subscription of Ubuntu Pro. Adding a subscription to Ubuntu pro provides security updates for an extended period of time. For more information, see Ubuntu Pro in the Canonical documentation.

Topics

- Eligible license types for license type conversion in License Manager
- Conversion prerequisites for License Manager license types
- Convert a license type in License Manager
- Tenancy conversion in License Manager
- Troubleshooting license type conversion in License Manager

Eligible license types for license type conversion in License Manager

You can use License Manager license type conversion with supported versions and combinations of Windows Server and Microsoft SQL Server licenses. You can also use license type conversion with Ubuntu Linux subscriptions.

Contents

- Eligible license types for Windows and SQL Server in License Manager
  - SQL Server editions
  - SQL Server versions
  - Usage operation values
  - Media compatibility
  - Conversion paths
- Eligible subscription types for Linux in License Manager
  - License type conversion considerations

Eligible license types for Windows and SQL Server in License Manager

> **Important**
>
> Instances that were originally launched from an Amazon provided Amazon Machine Image (AMI) are not eligible for license type conversion to BYOL.

Windows and SQL Server must meet certain requirements in order to be eligible for license type conversion.

Topics

- SQL Server editions
- SQL Server versions
- Usage operation values
- Media compatibility
- Conversion paths

SQL Server editions

License Manager supports the following SQL Server editions:

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

SQL Server versions

License Manager supports the following SQL Server versions:

- SQL Server 2005
- SQL Server 2008
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

- SQL Server 2019
- SQL Server 2022

Usage operation values

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

Operating system details	Usage operation
Windows Server as BYOL	RunInstances:0800
Windows Server as BYOL SQL Server (any edition) as BYOL	RunInstances:0800
Windows Server as license included	RunInstances:0002
Windows Server as license included SQL Server (any edition) as BYOL	RunInstances:0002
Windows Server as license included SQL Server Web as license included	RunInstances:0202
Windows Server as license included SQL Server Standard as license included	RunInstances:0006
Windows Server as license included SQL Server Enterprise as license included	RunInstances:0102

Media compatibility

The following table confirms which media can be used on which instance licensing models.

Source	Target	
	BYOL	License included
AWS provided Windows Server image	No	Yes
AWS provided SQL Server image	No	Yes
Your Windows Server media[1]	Yes	Yes
Your SQL Server media[2]	Yes	Yes

[1] Denotes that the instance was originally launched from your own imported virtual machine (VM). You can import your VM using a service such as VM Import/Export or AWS Application Migration Service.

[2] Denotes that you have sourced your own SQL Server installation media (.iso, .exe).

Conversion paths

The following table confirms if the source license model can be converted to another between BYOL and license included. For more information, see Convert a license type in License Manager.

Important

- Windows Server as BYOL with SQL Server as license included is an unsupported configuration.
- Conversions that are specified as "Not needed" won't change the usage operation value.

Source	Target					
	Windows Server as BYOL	Windows Server as license included	Windows Server as BYOL SQL Server as BYOL	Windows Server as license included SQL Server as BYOL	Windows Server as BYOL SQL Server as license included	Windows Server as license included SQL Server as license included
Windows Server as BYOL (your media)	Not needed	Yes	Not needed	Yes[1]	Unsupported	Yes[1]
Windows Server as license included (your media)	Yes[2]	Not needed	Yes[1,2]	Not needed[3]	Unsupported	Yes[1]
Windows Server as license included (AWS provided image)	No✗	Not needed	No✗	Not needed[3]	Unsupported	Yes[1]
Windows Server as	Not needed[4]	Yes	Not needed	Yes	Unsupported	Yes

Source	Target					
BYOL (your media)						
SQL Server as BYOL (your media)						
Windows Server as license included (your media)	Yes[2]	Not needed[4]	Yes[2]	Not needed	Unsupported	Yes
SQL Server as BYOL (your media)						
Windows Server as license included (AWS provided image)	No✗	Not needed[4]	No✗	Not needed	Unsupported	Yes
SQL Server as BYOL (your media)						

Source	Target					
Windows Server as BYOL (your media) SQL Server as license included	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
Windows Server as license included (AWS provided image or your media) SQL Server as license included (AWS provided image)	No✗	No✗	No✗	No✗	Unsupported	Not needed

Source	Target					
Windows Server as license included (your media)	Yes[2,5,6]	Yes[5]	Yes[2]	Yes	Unsupported	Not needed
SQL Server as license included (your media)						
Windows Server as license included (AWS provided image)	No✗	Yes[5]	No✗	Yes	Unsupported	Not needed
SQL Server as license included (your media)						

✗ You must deploy a new instance with an alternate configuration, as converting to the target license type(s) is not supported. For more information, see Media compatibility.

For other conversion scenarios, you might need to take the following steps to perform a license conversion:

[1] You must first **install** SQL Server before converting to BYOL for SQL Server.

[2] You must first modify your Windows configuration to use your own KMS server for license activation. For more information, see Convert Windows Server from license included to BYOL.

[3] You must first **install** SQL Server when you convert from a source without SQL Server to a target with SQL Server (regardless of the SQL Server license type).

[4] You must first **uninstall** SQL Server when you convert from a source with SQL Server to a target without SQL Server (regardless of the SQL Server license type).

[5] You must first **uninstall** SQL Server before converting to license-included SQL Server.

[6] You must first perform the steps for [2] and [5]. Once these steps are complete, you must convert the license type to Windows Server as license included, and then convert the license type once more to Windows Server as BYOL.

Eligible subscription types for Linux in License Manager

License type conversion is available for supported versions of Ubuntu. The supported versions include updates such as Ubuntu 18.04.1 LTS. When you convert a subscription to Ubuntu Pro, security updates are provided for an additional five years. For more information, see Ubuntu Pro in the Canonical documentation.

You can use license type conversion for long-term support (LTS) versions of Ubuntu, RHEL, and RHEL for SAP. You can switch subscriptions between AWS-provided and Red Hat-provided options from AWS Marketplace.

License type conversion considerations

Some of the considerations that license type conversion is subject to are listed as follows. This is not a comprehensive list and is subject to change.

RHEL and RHEL for SAP conversion

- If you're converting to subscriptions sold by Red Hat as an AMI listing on AWS Marketplace you must first subscribe to the Marketplace AMI listing before initiating the license conversion.
- For transitions to the Red Hat Subscriptions SaaS listing on AWS Marketplace you need to purchase subscriptions from Red Hat prior to conversion.
- If you have an annual Red Hat contract from AWS Marketplace you will not receive a refund for unused months when converting to another subscription type.

- To convert from RHEL for SAP sold by Red Hat in AWS Marketplace to RHEL for SAP sold by AWS in AWS Marketplace send a request to Support. For more information, see Creating a support case.

Ubuntu conversion

- The instance must be running Ubuntu LTS in order to convert the license type to Ubuntu Pro.
- You can't use license type conversion for a Ubuntu Pro subscription. To remove a Ubuntu Pro subscription, see Remove a Ubuntu Pro subscription.
- Ubuntu Pro is not available as a Reserved Instance. For savings with On-Demand Instance pricing, we recommend that you use Ubuntu Pro with Savings Plans. For more information, see Reserved Instances in the *Amazon EC2 User Guide* and What are Savings Plans? in the *Savings Plans User Guide*.
- To convert from Ubuntu Pro to Ubuntu LTS send a request to Support. For more information, see Creating a support case.

Conversion prerequisites for License Manager license types

To convert license types with License Manager, there are general and operating system specific prerequisites.

Topics

- General
- Windows
- Linux

General

You must meet the following general prerequisites before performing a license type conversion:

- Your AWS account must be onboarded to License Manager. See Get started with License Manager.
- The target instance must run on AWS. On-premises instances are not supported.
- The target instance must be in the stopped state before you convert the license type. For more information, see Stop and start your instance in the *Amazon EC2 User Guide*.

- If stop protection is enabled on the target instance, the conversion process will fail. For more information, see Troubleshooting license type conversion in License Manager.
- The target instance must be configured with AWS Systems Manager Inventory. For more information, see Setting up Systems Manager for EC2 instances and AWS Systems Manager Inventory in the *AWS Systems Manager User Guide*.
- Your user or role must have the following permissions:
  - `ssm:GetInventory`
  - `ssm:StartAutomationExecution`
  - `ssm:GetAutomationExecution`
  - `ssm:SendCommand`
  - `ssm:GetCommandInvocation`
  - `ssm:DescribeInstanceInformation`
  - `ec2:DescribeImages`
  - `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.

Windows

Windows instances must meet the following prerequisites:

- Instances that were originally launched from an Amazon provided Amazon Machine Image (AMI) are not eligible for license type conversion 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.

- To change your SQL Server license to BYOL, SQL Server must have been installed using your own media.

Linux

Linux instances must meet the following prerequisites:

RHEL

- If converting from AWS-provided subscriptions to subscriptions sold by Red Hat as an AMI listing on AWS Marketplace, you must first subscribe to the Marketplace AMI listing from Red Hat before initiating the license conversion.
- For transitions from AWS-provided subscriptions to the Red Hat Subscriptions SaaS listing on AWS Marketplace you'll need to purchase subscriptions from Red Hat prior to conversion.

RHEL for SAP

- For RHEL for SAP and Update Services conversions, instances must be launched from AWS Marketplace with a RunInstance:0010 usage operation and an attached AWS Marketplace product code.
- If converting from AWS-provided subscriptions to subscriptions sold by Red Hat as an AMI listing on AWS Marketplace, you must first subscribe to the Marketplace AMI listing from Red Hat before initiating the license conversion.
- For transitions from AWS-provided subscriptions to the Red Hat Subscriptions SaaS listing on AWS Marketplace you'll need to purchase subscriptions from Red Hat prior to conversion.

Ubuntu

- Instances must be running Ubuntu LTS.
- The Ubuntu Pro Client must be installed in your Ubuntu operating system.
  - Run the following command to confirm if the Ubuntu Pro Client is installed:

```
pro --version
```

- If the command is not found, or the version needs to be updated, run the following command to install the Ubuntu Pro Client:

```
apt-get update && apt-get dist-upgrade
```

- Instances must be able to reach multiple endpoints to activate their Ubuntu Pro subscription and receive updates. You must allow outbound traffic from your instance over TCP port 443 to reach the following endpoints:
  - **contracts.canonical.com** – Used for Ubuntu Pro activation.
  - **esm.ubuntu.com** – Used for APT repository access for most services.
  - **api.snapcraft.io** – Used for installing and running snaps.
  - **dashboard.snapcraft.io** – Used for installing and running snaps.
  - **login.ubuntu.com** – Used for installing and running snaps.
  - **cloudfront.cdn.snapcraftcontent.com** – Used for downloading from content development networks (CDNs).
  - **livepatch.canonical.com** – Used for downloading patches from the Livepatch server.

  For more information, see Ubuntu Pro Client network requirements in the Ubuntu Pro Client documentation and Network requirements in the Canonical Snapcraft documentation.

Convert a license type in License Manager

You can convert Windows licenses, Microsoft SQL Server licenses, and Ubuntu Linux subscriptions using the License Manager console or AWS CLI. You might need to complete additional steps to convert the license or subscription in the operating system of the instance.

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

License Manager might update the resources associated with your self-managed licenses as part of a license type conversion. Specifically, for any self-managed license with automated discovery rules of type `License Included`, License Manager disassociates the resource in the license

type conversion from the license if the `license included` automated discovery rule explicitly excludes the resource.

For example, if your self-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 self-managed license. However, if only one of the two automated discovery rules contains a `License Included` rule, then the instance is not disassociated.

You should not start or stop your instance while a license type conversion is in progress. When the license type conversion 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 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`.

Contents

- Convert a license type for Windows and SQL Server in License Manager
  - License type conversion limits
  - Convert a license type using the License Manager console
  - Convert a license type using the AWS CLI
- Convert a license type for Linux in License Manager
  - Convert a license type using the License Manager console
  - Convert a license type using the AWS CLI
  - Remove a Ubuntu Pro subscription

Convert a license type for Windows and SQL Server in License Manager

You can use either the License Manager Console or the AWS CLI to convert the license type of eligible Windows and SQL Server instances.

Topics

- License type conversion limits
- Convert a license type using the License Manager console
- Convert a license type using the AWS CLI

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 conversions 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 License Manager console

You can use the License Manager console to convert a license type.

> **Note**
>
> Only instances that are in a stopped state and have been associated by AWS Systems Manager Inventory are displayed.

To start a license type conversion in the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/ .
2. From the left navigation pane, choose **License type conversion**, then choose **Create license type conversion**.
3. For **Source operating system**, choose the platform of the instance you want to convert:
   - **RHEL**
   - **RHEL for SAP**
   - **Ubuntu LTS**
   - **Windows BYOL**
   - **Windows license included**
4. (Optional) Filter the available instances by specifying a value for **Instance ID** or **Usage operation value**.
5. Select the instances whose licenses you want to convert, and then choose **Next**.
6. Enter the **Usage operation value** for the license type, select the license that you are converting to, and choose **Next**.
7. Verify that you are satisfied with your license type conversion configuration and choose **Start conversion**.

You can view the status of your license type conversion from the license type conversion panel. The Conversion status column displays the status of the conversion as **In progress**, **Completed**, or **Failed**.

> **Important**
>
> If you convert Windows Server from license included to BYOL, you must activate Windows according to your Microsoft license agreement. See Convert Windows Server from license included to BYOL for more information.

Convert a license type using the AWS CLI

To start a license type conversion 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.

   Important

   You might need to update the AWS CLI to run certain commands and receive all required output in the following steps.

2. Verify that you have permissions to run the `create-license-conversion-task-for-resource` AWS CLI command. For help with this, see Create IAM policies for License Manager.

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-ids <instance-id> --query
    "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
    PlatformDetails, ProductCode: ProductCode, UsageOperation: UsageOperation,
    UsageOperationUpdateTime: UsageOperationUpdateTime}"
   ```

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": "i-0123456789abcdef",
   "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 Server 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 both Windows Server and SQL Server from BYOL to license included

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

To convert the license type of your Windows Server instance from BYOL to license included, 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:0800 \
 --destination-license-context UsageOperation=RunInstances:0006
```

Convert a license type for Linux in License Manager

You can use either the License Manager Console or the AWS CLI to convert the license type of eligible Ubuntu LTS, RHEL, and RHEL for SAP instances.

Topics

- Convert a license type using the License Manager console
- Convert a license type using the AWS CLI
- Remove a Ubuntu Pro subscription

Convert a license type using the License Manager console

You can use the License Manager console to convert a license type.

> **Note**
>
> Only instances that are in a stopped state and have been associated by AWS Systems Manager Inventory are displayed.

To start a license type conversion in the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/ .
2. From the left navigation pane, choose **License type conversion**, then choose **Create license type conversion**.
3. For **Source operating system**, choose the platform of the instance you want to convert:
   - **RHEL**
   - **RHEL for SAP**
   - **Ubuntu LTS**
   - **Windows BYOL**
   - **Windows license included**
4. (Optional) Filter the available instances by specifying a value for **Instance ID** or **Usage operation value**.
5. Select the instances whose licenses you want to convert, and then choose **Next**.
6. Enter the **Usage operation value** for the license type, select the license that you are converting to, and choose **Next**.
7. Verify that you are satisfied with your license type conversion configuration and choose **Start conversion**.

You can view the status of your license type conversion from the license type conversion panel. The Conversion status column displays the status of the conversion as **In progress**, **Completed**, or **Failed**.

Convert a license type using the AWS CLI

To start a license type conversion in the AWS CLI, you should confirm the license type of your instance is eligible, and then perform a license type conversion to change to the required subscription. For more information on eligible subscription types, see Eligible subscription types for Linux in License Manager.

Determine the license type of your instance

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.

> **Important**
>
> You might need to update the AWS CLI to run certain commands and receive all required output in the following steps. Verify that you have permissions to run the `create-license-conversion-task-for-resource` AWS CLI command. For more information, see Create IAM policies for License Manager.

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-ids <instance-id> --query
 "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
 PlatformDetails, UsageOperation: UsageOperation, UsageOperationUpdateTime:
 UsageOperationUpdateTime}"
```

The following is an example response to the `describe-instances` command. The **UsageOperation** value is the billing information code associated with the license. A usage operation value of `RunInstances` indicates that the instance is using AWS provided licensing. The `UsageOperationUpdateTime` is the time when the billing code was updated. For more information, see DescribeInstances in the *Amazon EC2 API Reference*.

```
"InstanceId": "i-0123456789abcdef",
"Platform details": "Linux/UNIX",
"UsageOperation": "RunInstances",
"UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
```

Convert to Ubuntu Pro

Before you convert your instance from Ubuntu LTS to Ubuntu Pro, your instance must have outbound internet access configured to retrieve a license token from the Canonical servers and install the Ubuntu Pro Client. For more information, see Conversion prerequisites for License Manager license types.

To convert Ubuntu LTS to Ubuntu Pro, follow these steps:

1. Run the following command from the AWS CLI while specifying your instance's ARN:

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances \
    --destination-license-context UsageOperation=RunInstances:0g00
```

2. Run the following command from within the instance to retrieve details about your Ubuntu Pro subscription status:

```
pro status
```

3. Confirm your output indicates that the instance has a valid Ubuntu Pro subscription:

```
ubuntu@ip-                    pro status
SERVICE                       STATUS    DESCRIPTION
cc-eal           yes          disabled  Common Criteria EAL2 Provisioning Packages
cis              yes          disabled  Security compliance and audit tools
esm-apps         yes          disabled  Expanded Security Maintenance for Applications
esm-infra        yes          enabled   Expanded Security Maintenance for Infrastructure
fips             yes          disabled  NIST-certified core packages
fips-updates     yes          disabled  NIST-certified core packages with priority security updates
livepatch        yes          enabled   Canonical Livepatch service

Enable services with: pro enable <service>

               Account:
          Subscription:
           Valid until: Fri Dec 31 00:00:00 9999 UTC
Technical support level: essential
```

Remove a Ubuntu Pro subscription

License type conversion can only be used to convert from Ubuntu LTS to Ubuntu Pro. If you need to convert from Ubuntu Pro to Ubuntu LTS, you will need to raise a request to Support. For more information, see Creating a support case.

Tenancy conversion in License Manager

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

Your account must have a Dedicated Host with available capacity to start the instance in order to switch to the Dedicated Host tenancy type. For more information about working with dedicated hosts, see Work with Dedicated Hosts in the *Amazon Elastic Compute Cloud User Guide*.

To move to the host resource groups tenancy type, you must have at least one host resource group in your account. In order to launch an instance into a host resource group, the instance must have the same set of licenses that are associated with the host resource group. For more information, see Host resource groups in License Manager.

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 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 in License Manager

Troubleshooting topics

- Windows activation
- Instance [instance] is launched from an Amazon owned AMI. Provide an instance launched originally from a BYOL AMI.
- Failed to validate that instance [instance] was launched from a BYOL AMI. Ensure that the SSM Agent is running on your instance.
- An error occurred (InvalidParameterValueException) when calling the CreateLicenseConversionTaskForResource operation: ResourceId - [instance] is in an invalid state for changing license type.

- EC2 instance [instance] failed to stop. Ensure that you have permissions for EC2 StopInstances.

Windows activation

A license type conversion contains 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.

Instance [instance] is launched from an Amazon owned AMI. Provide an instance launched originally from a BYOL AMI.

You must launch your Amazon EC2 Windows instance from an AMI that you have imported to perform a license type conversion to Bring Your Own License model (BYOL). Instances originally launched from an Amazon-owned AMI aren't eligible for license type conversion to BYOL. For more information, see Conversion prerequisites for License Manager license types.

Failed to validate that instance [instance] was launched from a BYOL AMI. Ensure that the SSM Agent is running on your instance.

In order for the license type conversion to succeed, your instance must first have been online and managed by Systems Manager to have its inventory collected. The AWS Systems Manager Agent (SSM Agent) will gather inventory from your instance, which includes details about the operating system. For more information, see Checking SSM Agent status and starting the agent and Troubleshooting SSM Agent in the *AWS Systems Manager User Guide*.

An error occurred (InvalidParameterValueException) when calling the `CreateLicenseConversionTaskForResource` operation: ResourceId - [instance] is in an invalid state for changing license type.

To perform a license type conversion, the target instance must be in the stopped state. For more information, see Conversion prerequisites for License Manager license types and Troubleshoot stopping your instance in the *Amazon Elastic Compute Cloud User Guide*.

EC2 instance [instance] failed to stop. Ensure that you have permissions for EC2 `StopInstances`.

You must have permissions to perform the `StopInstances` EC2 API action on the target instance. Also, If stop protection is enabled on the target instance, the conversion process will fail. For more information, see Disable stop protection for a running or stopped instance in the *Amazon Elastic Compute Cloud User Guide*.

Host resource groups in License Manager

Amazon EC2 Dedicated Hosts are physical servers 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. For more information, see Dedicated Hosts in the *Amazon EC2 User Guide*.

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 self-managed licenses** – The self-managed licenses that can be used to launch instances in this host resource group.
- **(Optional) 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 in License Manager
- Share a host resource group in License Manager
- Add Dedicated Hosts to a host resource group in License Manager
- Launch an instance in a host resource group in License Manager
- Modify a host resource group in License Manager
- Remove Dedicated Hosts from a host resource group in License Manager
- Delete a host resource group in License Manager

Create a host resource group in License Manager

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 self-managed licenses with your host resource group. To best optimize host utilization, you can allow all core- or socket-based self-managed licenses 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 **self-managed licenses**, select one or more core- or socket-based self-managed licenses.

8. (Optional) For **Tags**, add one or more tags.
9. Choose **Create**.

Share a host resource group in License Manager

You can use AWS Resource Access Manager to shared your host resource groups through AWS Organizations. After you share a host resource group and self-managed license, 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.

Add Dedicated Hosts to a host resource group in License Manager

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 self-managed licenses and instances types, the host you add must match these requirements.

> **Note**
>
> If you stop instances and want to restart them, you must perform the following two tasks:
>
> - Modify the instance to point to the host resource group.
> - Associate self-managed licenses to match the host resource group.

There is no limit to the number of Dedicated Hosts that you can add to a 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.**

Launch an instance in a host resource group in License Manager

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 self-managed license 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 in License Manager

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**.

Remove Dedicated Hosts from a host resource group in License Manager

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. To work with a Dedicated Host that has been removed from a host resource group, see Work with Dedicated Hosts in the *Amazon EC2 User Guide*.

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.

Delete a host resource group in License Manager

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**.

Inventory search 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 **Inventory search** 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 License Manager.

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

- Work with inventory search in License Manager
- Automated discovery of inventory in License Manager

Work with inventory search in License Manager

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

Tasks

- Set up for inventory search
- Use inventory search
- Add automated discovery rules to a self-managed license
- Associate a self-managed license with inventory search
- Disassociate a self-managed license and a resource

Set 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.
- Create self-managed licenses for the servers and applications to manage. For example, create a self-managed license that reflects the terms of your licensing agreement with Microsoft for SQL Server Enterprise.

Use 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").

Search your resource inventory

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Inventory search**.
3. (Optional) You can specify filter options to streamline search results as follows.

   Amazon EC2 resources

Filter name	Description	Logical operators	Supported values
Resource ID	The ID of the resource.	`Equals`, `Not equals`	
Account ID	The ID of the AWS account that owns the resource.	`Equals`, `Not equals`	
Platform name	The operating system platform for the resource.	`Equals`, `Not equals`, `Begins with`, `Contains`	

Filter name	Description	Logical operators	Supported values
Application name	The name of the application.	`Equals`, `Begins with`	
License included name	The type of license included.	`Equals`, `Not equals`	• `SQL Server Enterprise` • `SQL Server Standard` • `SQL Server Web` • `Windows Server Datacenter`
Tag	A metadata tag key and optional value that's assigned to the resource. Note, the `Not equals` logical operator is only available if cross-account discovery is enabled.	`Equals`, `Not equals`	

Amazon RDS resources

Filter name	Description	Logical operators	Supported values
Engine Edition	The database engine edition.	`Equals`	• `oracle-ee` • `oracle-se` • `oracle-se1` • `oracle-se2` • `db2-se` • `db2-ae`

Filter name	Description	Logical operators	Supported values
License Pack (Oracle only)	The management pack associated with an Amazon RDS for Oracle license.	`Equals`	• `Spatial and Graph` • `Active Data Guard` • `Label Security` • `Oracle On-Line Analytical Processing (OLAP)` • `Diagnosti c Pack and Tuning Pack`

For more information about Amazon RDS database product licenses, see RDS for Oracle licensing options, or RDS for Db2 licensing options in the *Amazon RDS User Guide*.

Add automated discovery rules to a self-managed license

After you add product information to your self-managed license, License Manager can track license usage for the instances that have those products installed. For more information, see Automated discovery of inventory in License Manager.

To add automated discovery rules to a self-managed license

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Open the **Inventory search** page.
3. Select the resource and choose **Add automated discovery rules**.
4. For **Self-managed license**, select a self-managed license.

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 exclude resources from automated discovery select **Add exclusion rule**.

   > **Note**
   >
   > Exclusion rules do not apply to Amazon RDS products (such as RDS for Oracle and RDS for Db2).

   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**.

Associate a self-managed license with inventory search

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

To associate a self-managed license with a resource

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Open the **Inventory search** page.
3. Select the resource and choose **Associate self-managed license**.
4. For **self-managed license name**, select a self-managed license.
5. (Optional) Select **Share self-managed license with all my member accounts**.
6. Choose **Associate**.

Disassociate a self-managed license and a resource

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

To disassociate a self-managed license and a resource

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

Automated discovery of inventory in License Manager

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 self-managed license, 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 self-managed license, 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 self-managed license and create a new one.

To use automated discovery, you must add product information to your self-managed license. You can do so when you create the self-managed license using **Inventory search**.

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 search by integrating License Manager with your AWS Organizations account. For more information, see Settings in License Manager.

> **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 self-managed license

You can configure automated discovery rules and exclusion rules when you create a self-managed license. For more information, see Create a self-managed license in License Manager.

To add automated discovery rules to an existing self-managed license

Use the process below to add automated discovery rules to existing self-managed licenses through the console, you can also do this from the **Inventory search** 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 **Self-managed licenses**.
3. Choose the name of the self-managed license 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.

> **Note**
>
> The following limitations apply to Amazon RDS database products (such as Amazon RDS for Oracle and Amazon RDS for Db2):
>
> - A maximum of one rule specifying an Amazon RDS database product is supported.
> - Only one license configuration is allowed for each Amazon RDS database product.

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 database products (such as Amazon RDS for Oracle and Amazon RDS for Db2).
   > - Exclusion rules are only available if Cross-account resource discovery has been enabled.

   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.

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.

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.

Topics

- View your granted licenses
- Manage your granted licenses in License Manager
- Distribute License Manager entitlements
- Grant acceptance and activation in License Manager
- License status for grants in License Manager
- CloudWatch metrics for buyer accounts in License Manager

View your granted licenses

License Manager displays tabs to view and manage your granted licenses based on the permissions you are authenticated with. The granted license page can display the following tabs:

My licenses

This tab is available for any user that has access to view the granted licenses in License Manager. The tab has a **My granted licenses** section which includes information about each license such as the **License ID** and **Product name**. From this page you can view additional information about each license.

License summary (for organization administrators)

This tab is available only for organization administrators. The tab has a **Totals** section which lists the total amount of products and granted licenses across all accounts in your organization. It also shows a **Products** section which includes a table detailing the properties of each product, such as the **Product name** and **Number of granted licenses**.

Aggregated licenses (for organization administrators)

This tab is available only for organization administrators. This tab has a section detailing **Granted licenses for my organization** which includes information about each license such as the **License ID** and **Product name**. From this page you can view additional information about each license.

Manage your granted licenses in License Manager

Licenses that have been granted to you will 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 AWS 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 are automatically accepted and activated.
- If the management account for an organization with all features enabled purchases a subscription 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 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 use License Manager to distribute licenses.
- If the management account for an organization with all features enabled purchases a product 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 and distributes licenses to member accounts, each member account must accept and activate the license.

Console (My licenses)

You can view and manage granted licenses for a single AWS account.

To manage granted licenses in your account

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.

2. In the navigation pane, choose **Granted licenses**.
3. Choose the **My licenses** tab if it is not the current selection.
4. (Optional) Use the filter options, such as the following, to scope the list of licenses that are displayed.
   - Product SKU – The product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs.
   - Recipient – The ARN of the license recipient.
   - Status – The status of the license. For example, **Available**.
5. To view additional information about the license, choose the license ID to open the **License overview** page.
6. 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.

If you don't want to continue using a license that was activated, you can return to the **License overview** page and choose **Deactivate license**. If you want to continue using a license that was deactivated, return to the **License overview** page and choose **Activate license**.

Console (Aggregated licenses)

You can view your granted licenses that have been aggregated from all accounts in your organization.

> **Important**
>
> In order to use the organization wide view for your granted licenses, you must first link AWS Organizations using the AWS License Manager console settings. For more information, see Settings in License Manager.

To manage granted licenses across your accounts in AWS Organizations

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. Choose the **Aggregated licenses** tab if it is not the current selection.
4. (Optional) Use the filter options, such as the following, to scope the list of licenses that are displayed.

   - Product SKU – The product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs.
   - Beneficiary – The account in your organization that the license is granted to.
5. To view additional information about the license, choose the license ID to open the license detail page.
6. If the license issuer is an entity other than AWS Marketplace, do one of the following:
   - Choose **Activate license**. The resulting grant status is **Active**.
   - Choose **Deactivate license**. The resulting grant status is **Deactivated**.

If you don't want to continue using a license that was activated, you can return to the **License overview** page and choose **Deactivate license**. If you want to continue using a license that was deactivated, return to the **License overview** page and choose **Activate license**.

AWS CLI

You can use the AWS CLI to work with your granted licenses.

To manage your granted licenses using the AWS CLI:

- accept-grant
- create-grant-version
- get-grant
- list-licenses
- list-received-grants
- list-received-grants-for-organization
- list-received-licenses
- list-received-licenses-for-organization
- reject-grant

Distribute License Manager entitlements

If you are a license administrator operating in the management account of your organization with all features enabled, you can distribute entitlements to your organization from your granted licenses by creating a grant. For more information about AWS Organizations, see AWS Organizations terminology and concepts.

You can specify the recipient of the grant as one of the following:

- An AWS account, which includes only the specified account.
- An organization root, which will include all accounts across your organization.
- An organizational unit (OU) (that is not nested), which includes all accounts in the specified OU and in nested OUs under the specified OU.

> **Note**
>
> You can create up to 2,000 grants per license.

You can use either the AWS License Manager console or the AWS CLI to distribute your entitlements. You can specify the organization ID or the organization ARN when creating a grant in the console, but the ARN format must be used with the AWS CLI. For example, the ARNs will resemble the following:

Organization ID ARN

```
arn:aws:organizations::<account-id-of-management-account>:organization/
o-<organization-id>
```

Organization OU ARN

```
arn:aws:organizations::<account-id-of-management-account>:ou/
o-<organization-id>/ou-<organizational-unit-id>
```

Console

To create a grant (Console)

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 overview** 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, AWS Organizations OU ID or ARN, or AWS Organizations ID or ARN of the grant recipient.
    c. Choose **Create grant**.
6. On the **License overview** 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.

AWS CLI

You can use the AWS CLI to distribute an entitlement. You must use specify an organization ID or OU in ARN format when using the AWS License Manager API.

To create and list your grants using the AWS CLI:

- create-grant
- list-distributed-grants

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.

Grant acceptance and activation in License Manager

When a grant is created for a granted license, it is distributed to the recipient. A granted license must be accepted and activated before it can be used by the grant recipient. The grant activation process can include additional options for granted licenses sourced from the AWS Marketplace.

By default, the **Grant overview** page for a granted license has a status of `Pending Acceptance`. You can choose to `Accept`, `Accept and Activate`, or `Reject` the grant. Grants that are accepted but not yet activated have a status of `Disabled`. Accepted and activated grants have a status of `Active`.

A granted license must be accepted and activated before it can be used by the grant recipient. 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. Grants that are accepted but not yet activated have a status of **Disabled**. Accepted and activated grants have a status of **Active**.

> **Tip**
>
> You can automatically accept grants that come from the management account of your organization. To enable grant auto-acceptance, link your organization accounts on the settings page in the AWS License Manager console from the management account.

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 can take one of the following actions:

1. Disable the existing grant for the same product and then activate the new grant.
2. Activate the new grant and specify that you want to disable and replace the existing active grant with the new grant. You can use the License Manager console or the AWS CLI:
   a. Using the License Manager console, activate the new grant while selecting **Yes** that you want to replace active grants.
   b. Using the `CreateGrantVersion` API, activate the new grant by specifying `ALL_GRANTS_PERMITTED_BY_ISSUER` for the `ActivationOverrideBehavior` with a `Status` of `Active`.

Console

You can use the License Manager console to activate a grant. When you activate a grant sourced from the AWS Marketplace, you might be presented with the option whether to replace active grants:

- As a license administrator, you must specify if you want to replace active grants when activating a grant.

- As a grantor, you can optionally specify if you want to replace active grants when you activate a grant for another account in your organization.

- As a grantee, if the grantor creating the distributed grant didn't specify whether to replace active grants, you must make a selection when activating the grant.

To activate a grant (Console)

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 overview** page.
4. Choose a grant name to open the **Grant overview** page.
5. If presented, select an activation option for whether you want to replace active grants:
   a. **No** – This option will activate the grant without replacing any existing active grants for the recipient (grantee).
   b. **Yes** – This option will disable grants for the same product and activate a new grant for the defined recipient (grantee):
      i. A specified AWS account.
      ii. Member accounts of the specified organization OU.
      iii. All member accounts of the organization.
6. (Optional) Provide a reason for activating the grant.
7. Enter **`activate`** into the input box, and choose **Activate**.

AWS CLI

You can use the AWS CLI to work with your granted licenses.

To work with distributed grants using the AWS CLI:

- accept-grant
- create-grant-version
- list-received-grants
- list-received-grants-for-organization
- reject-grant

License status for grants in License Manager

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.

The follow table shows the various statuses for a granted license:

Status	Description
AVAILABLE	The license is available to use and share.
PENDING_AVAILABLE	The license is not available to use as it is still processing.
DEACTIVATED	The license is not available to use because it has been deactivated by the license issuer.
SUSPENDED	The license is not available to use as it is suspended.
EXPIRED	The license is not available to use because it has reached the end of term.
PENDING_DELETE	The license is not available to use as it is in the process of being deleted.
DELETED	The license is not available to use because the license agreement has been canceled.

The following table shows the various statuses for a grant:

Status	Description
PENDING_WORKFLOW	The grant is in the process of being distribut ed.
PENDING_ACCEPT	The grant has been created and the grant recipient has not yet accepted it.

Status	Description
REJECTED	The grant has been rejected by the grant recipient.
ACTIVE	The grant has been accepted and activated for use by the grant recipient. The licensed resource can be used.
FAILED_WORKFLOW	The grant failed to distribute.
DELETED	The grant has been deleted by the grantor.
PENDING_DELETE	The grant that was distributed is in the process of being deleted.
DISABLED	The grant has been accepted by the grant recipient, but has not been activated for use.
WORKFLOW_COMPLETE	The grant to an organization has been distributed or recalled. The grant details show the status of sub-grants to each account in the organization.

CloudWatch metrics for buyer accounts in License Manager

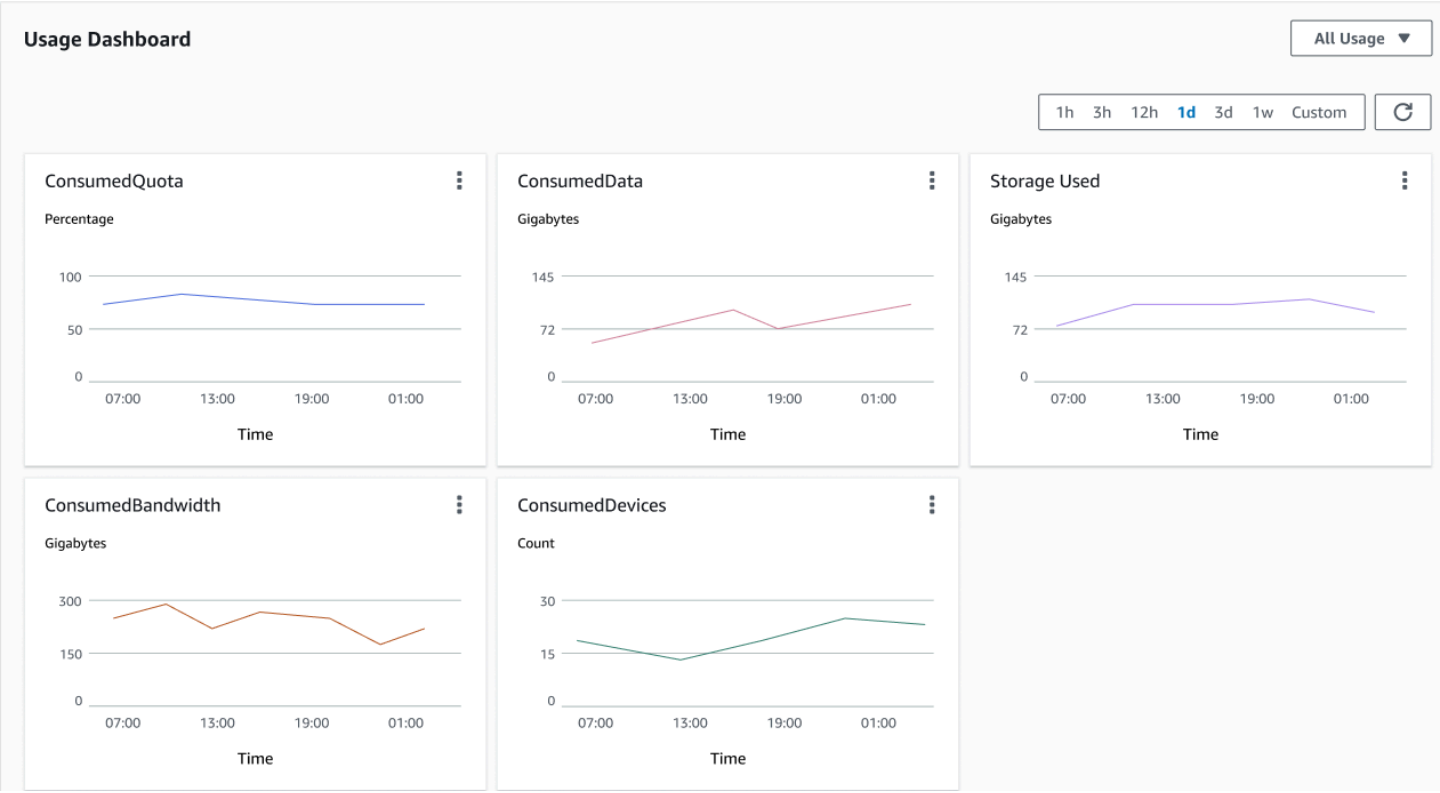
When a grant for a seller issued license is configured with **allow submission of usage records** selected, License Manager emits a CloudWatch metric to the seller account, root buyer account, and the account against which the usage is being recorded. Buyer accounts are the AWS accounts who have purchased or been granted a seller issued license. For more information, see Granting licenses to customers.

Usage dashboard

When a seller or independent software vendor (ISV) application records usage against a license for a buyer account, the account in which usage is being recorded and the root buyer account see a CloudWatch widget with usage records on the **Usage dashboard** page in the License Manager console. Buyers can also see metrics for accounts that they have distributed licenses to in AWS

Organizations. The graphs on the **Usage dashboard** page are available for every license for which usage records have been sent.

The following image is an example of the usage dashboard:



Seller issued licenses in 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 the licenses you issue 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 your customers with an AWS IAM identity or through bearer tokens generated by License Manager. ISV 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.

Seller issued license entitlements in License Manager

License Manager captures seller issued 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.

Seller issued license usage in License Manager

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.

Permissions required to track seller issued license usage in License Manager

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

JSON

```
{
    "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 an IAM role that enables your software application to call the License Manager API.

If you use the AWS Management Console to distribute temporary credentials for customers without an AWS account, License Manager will automatically create the `AWSLicenseManagerConsumptionRole` on your behalf. For more information, see Get temporary credentials for ISV customers without an AWS account. To create this role from the AWS CLI, use the AWS IAM create-role command, as shown in the following example.

```
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 provided `trust-policy-document.json` file should look like the following example, with your own AWS account ID substituted as the token issuer account.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "openid-license-manager.amazonaws.com"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "openid-license-manager.amazonaws.com:amr": "aws:license-
manager:token-issuer-account-id:123456789012"
                }
            }
        }
    ]
```

```
}
```

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
```

Create seller issued licenses in License Manager

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 in License Manager.
   - **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**.

Grant License Manager seller issued licenses to ISV 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.

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

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**
     - Select **Consumption** if the recipient can consume granted entitlements.
     - Select **Distribution** if the recipient can distribute granted entitlements to other AWS accounts.
     - Select **Allow on-premise token generation** to authenticate shared licenses without using AWS identities or credentials.
     - Select **Allow submission of usage records** to permit license recipients to emit usage records for usage types.
   - **Home Region** – The AWS Region for the license.
6. Choose **Create grant**.

Get temporary credentials for ISV customers without an AWS account

For customers without an AWS account, you can use entitlements in the same manner 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.

To create a token from the AWS License Manager console

1. From the License Manager console, navigate to the License details page for the specific license entitlement you want to use without an AWS account.

2. Choose **Create token** to generate a temporary access token.

> **Note**
>
> The first time you generate a temporary access token, you will be asked to create a service role so that License Manager can access services on your behalf. The following service role is created: `AWSLicenseManagerConsumptionRole`.

3. Download the `token.csv` file, or copy the token string when it is generated.

> **Important**
>
> This is the only time you can view or download this token. We recommend that you download the token and store the file in a secure location. You can create new tokens at any time, up to the service limit.

Check out seller issued licenses in License Manager

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

Delete seller issued licenses in License Manager

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**.

Use License Manager user-based subscriptions for supported software products

With user-based subscriptions in AWS License Manager, you can purchase fully-compliant licensed software subscriptions. Licenses are provided by Amazon and have a per-user subscription fee. Amazon EC2 provides pre-configured Amazon Machine Images (AMIs) with the supported software,

along with license-included Windows Server licenses. These licenses can be used without long-term licensing commitments.

To use user-based subscriptions, you associate users from AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD), or from your self-managed (on-premises) domain, with EC2 instances providing the software. To make your licensed software available, you must create user-based subscriptions and associate them with instances launched from pre-configured AMIs. AWS Systems Manager will configure and harden the license-included instances you launch. Users must connect with Remote Desktop software to access the instances providing the software.

Each associated user and vCPU for the license-included instances incur charges. Amazon EC2 Reserved Instances and Savings Plan pricing models can help optimize your Amazon EC2 costs. For more information, see Reserved Instances in the *Amazon Elastic Compute Cloud User Guide*. User-based subscriptions are billed from the first half of the month to the end of the month.

Topics

- Considerations for using user-based subscriptions in License Manager
- Subscription charges in License Manager
- Prerequisites to create user-based subscriptions in License Manager
- Supported software products for user-based subscriptions in License Manager
- Active Directory
- Additional software
- Get started with user-based subscriptions in License Manager
- Configure Active Directory GPO for more active remote user sessions
- Launch an instance from a license included AMI
- Connect to a user-based subscription instance with RDP
- Modify firewall settings for your Microsoft Office subscription
- Manage subscription users for License Manager user-based subscriptions
- Deregister an Active Directory from License Manager settings
- Troubleshoot user-based subscriptions in License Manager

Considerations for using user-based subscriptions in License Manager

The following considerations apply when using user-based subscriptions with License Manager:

- The AWS Marketplace subscription for license-included Microsoft Remote Desktop Services (`Win Remote Desktop Services SAL`) has a per user per month fee, with no proration.
- Instances that provide user-based subscriptions support up to two active user sessions at a time by default. To enable more than two active user sessions, you can configure an Active Directory Group Policy Object (GPO), and set the Microsoft RDS licensing mode to `Per User`. For more information, see the prerequisites for Configure Active Directory GPO for more active remote user sessions.
- When you create local users with administrator privileges on instances that provide user-based subscriptions, the instance health status might change to unhealthy. License Manager can terminate instances that are unhealthy for non-compliance. For more information, see Troubleshooting instance compliance.
- When you configure your Active Directory with Microsoft Office products, your VPC must have VPC endpoints provisioned in at least one subnet. If you want to remove all VPC endpoint resources created by License Manager, you must remove any Active Directory that's configured from the License Manager settings. For more information, see Deregister an Active Directory from License Manager settings.
- The tag key of `AWSLicenseManager` with the value of `UserSubscriptions` assigned by License Manager to your instances must not be altered or deleted.
- For the service to function as expected the two network interfaces created for License Manager must not be altered or deleted.
- The objects that License Manager creates in the AWS Managed Microsoft AD directory's **AWS Reserved** organizational unit (OU) must not be altered or deleted.
- The instances deployed for user-based subscriptions must be managed nodes with AWS Systems Manager and joined to the same domain. For information on keeping your instances managed by Systems Manager, see the Troubleshoot user-based subscriptions in License Manager section of this guide.
- To stop incurring Microsoft Office or Visual Studio subscription charges for a user, you must disassociate the user from all instances they are associated with. For more information, see Disassociate users from an instance that provides License Manager user-based subscriptions.

Subscription charges in License Manager

Subscription and billing in License Manager varies based on the subscription product that's used.

Microsoft Office and Visual Studio subscriptions

For Microsoft Office and Visual Studio subscriptions, billing stops as soon as you have disassociated the user from all instances that provide the subscription product, and unsubscribed them from the product.

Microsoft Remote Desktop Services (RDS) subscriptions

Microsoft RDS is billed on a per user, per month basis based on a combination of the user subscription and the client access license (CAL) token that's issued from the license server when the user connects to an instance that provides the subscription product.

Microsoft RDS billing in License Manager

Microsoft RDS billing begins when the Active Directory user is subscribed through License Manager, and ends after the client access license (CAL) token expires, 60 days from the date it's issued, with no proration for partial months. Billing continues until the token expires, even if you unsubscribe the user.

If an unsubscribed user continues to log in after the license token expires, they are automatically re-subscribed, and billing continues until they are again unsubscribed and their token expires.

Similarly, if a user who has never subscribed, but logs into an instance that is associated with the license server, License Manager automatically subscribes them and begins RDS billing. Billing continues until they are unsubscribed and their token expires.

To stop billing for a user at the end of the current month, you must remove that user from the Active Directory that's configured for the license server before unsubscribing.

> **Warning**
>
> If you remove an Active Directory user who still has an active Microsoft Office or Visual Studio subscription, that user will no longer be able to access instances that they are associated with.

The following example scenarios demonstrate how RDS billing works.

Scenario 1: Standard subscription and billing

The following scenario shows a standard set of actions that affect billing for an Active Directory (AD) user who is subscribed on 12/15/2024, but never accesses a subscription instance.

Action: If the user never unsubscribes, billing continues indefinitely.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
12/15/2024	12/15/2024	--	N/A	--	--	--

Action: The user is unsubscribed on 1/15/2025.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
12/15/2024	12/15/2024	--	N/A	1/15/2025	No	1/31/2025

Scenario 2: How the license token affects user subscription and billing

The following scenario shows how the license token expiration affects the user subscription for an Active Directory (AD) user who is subscribed on 9/15/2024 and logs into a domain-joined subscription product instance the same day.

Action: Initial subscription and login for AD user.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

Action: The same AD user is unsubscribed on 10/19/2024. However, since the user wasn't removed from the directory, billing continues until the end of the month during which the license token expires.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

Alternative action: The AD administrator removes the user from the directory on 10/20/2024, and then unsubscribes the user on the following day. In this case, billing stops at the end of the month during which the user is removed from the directory.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/21/2024	10/20/2024	10/31/2024

Scenario 3: Unsubscribed user is resubscribed

The following scenario shows how an unsubscribed Active Directory (AD) user whose license token has expired is automatically resubscribed when they access a domain-joined subscription product instance.

Action: Initial subscription and login for AD user.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

Action: The same AD user is unsubscribed on 10/19/2024. However, since the user wasn't removed from the directory, billing continues until the end of the month during which the license token expires.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

Action: The same AD user accesses a domain-joined subscription product instance after their previous license token expires but before billing ends. Billing continues until the user is unsubscribed again and their new token expires.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
11/20/2024 (re-subscribed)	billing continues	11/20/2024	1/20/2025	--	--	--

Scenario 4: Automatic subscription on instance access

The following scenario shows how an Active Directory (AD) user who was never subscribed to RDS SAL is automatically subscribed when they log into a domain-joined subscription product instance.

Action: An AD user who was never subscribed to RDS SAL logs into a domain-joined subscription product instance on 9/15/2024, and is auto-subscribed. Billing begins, and continues until the user is unsubscribed and their new token expires.

AD user subscribed	Billing starts	CAL issued	CAL expires	User unsubscribed	User removed from AD	Billing ends
9/15/2024 (auto-subscribed)	9/15/2024	9/15/2024	11/15/2024	--	--	--

For more information about how Microsoft RDS per user CALs work, see the **Per User CALs** section in the License your Remote Desktop deployment article on the *Microsoft Learn* website.

Prerequisites to create user-based subscriptions in License Manager

The following prerequisites must be implemented in your environment before you can create user-based subscriptions.

Contents

- IAM roles and permissions
  - AWS KMS Key policy for License Server credentials
- Active Directory
- Security groups
- Network configuration
- Instances that provide user-based subscription products
- Microsoft Remote Desktop Services
  - Administrative credentials secret

IAM roles and permissions

You must allow License Manager to create a service-linked role in order to onboard your AWS account for user-based subscriptions. In the License Manager console, a prompt appears in **User-based subscriptions** if the role hasn't been created yet. After you respond to the prompt and agree to allow License Manager to create the role, choose **Create** to continue. For more information, see Using service-linked roles for License Manager.

To create user-based subscriptions, your user or role must have the following permissions:

- **Amazon EC2** – Work with network interfaces and subnets.
  - `ec2:CreateNetworkInterface`
  - `ec2:DeleteNetworkInterface`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:CreateNetworkInterfacePermission`
  - `ec2:DescribeSubnets`
- **AWS Directory Service** – Administer Active Directories.
  - `ds:DescribeDirectories`
  - `ds:AuthorizeApplication`
  - `ds:UnauthorizeApplication`
  - `ds:GetAuthorizedApplicationDetails`
  - `ds:DescribeDomainControllers`
- **Route 53** – Configure routing.
  - `route53:DeleteHealthCheck`
  - `route53:ChangeResourceRecordSets`
  - `route53:GetHostedZone`
  - `route53:ListHostedZonesByName`
  - `route53:ListHostedZones`
  - `route53:ListHostedZonesByVPC`
  - `route53:CreateHostedZone`
  - `route53:DeleteHostedZone`
  - `route53:ListResourceRecordSets`
  - `route53:GetHealthCheckCount`

- route53:AssociateVPCWithHostedZone

To create user-based subscriptions for Microsoft Office products, your user or role must also have these additional permissions:

- ec2:CreateVpcEndpoint
- ec2:DeleteVpcEndpoints
- ec2:DescribeVpcEndpoints
- ec2:ModifyVpcEndpoint
- ec2:DescribeSecurityGroups

AWS KMS Key policy for License Server credentials

To use your own KMS key to encrypt and decrypt the administrative credentials secret for Microsoft RDS License Server, you must attach a policy to the role that you use for accessing License Manager operations. The following example shows a policy that grants permission for Secrets Manager to access the KMS key to encrypt and decrypt the Microsoft RDS License Server credential secret.

JSON

```
{
"Version": "2012-10-17",
"Id": "key-policy",
"Statement": [
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/RoleName"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "secretsmanager.*.amazonaws.com"
```

```
            }
        }
    },
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/aws-
service-role/license-manager-user-subscriptions.amazonaws.com/
AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService"
        },
        "Action": "kms:Decrypt",
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "secretsmanager.*.amazonaws.com"
            }
        }
    }
]
}
```

Active Directory

To use License Manager user-based subscriptions, you must create an Active Directory (AD) that contains user information for the subscription product users. Depending on your configuration, you can use an AWS Managed Microsoft AD, or a self-managed AD.

If you use both AWS managed and self-managed Active directories, you must establish a two-way forest trust between the directories. For more information, see Tutorial: Create a trust relationship between your AWS Managed Microsoft AD and your self-managed Active Directory domain in the *AWS Directory Service Administration Guide*.

> **Note**
>
> Subnets that are configured for your directory must all be from the same VPC for your AWS account. Shared subnets are not supported.

AWS managed Active Directories have the following restrictions.

- Directories that are shared with you aren't supported.
- Multi-factor authentication is not supported

Prerequisite for tag-based filters

If you will use tag-based filters for your Active Directory, you must first onboard to the AWS Resource Explorer service, as follows:

1. Open the Resource Explorer console at https://resource-explorer.console.aws.amazon.com/resource-explorer.
2. Choose **Turn on Resource Explorer**.
3. In the **Set up Resource Explorer** page, choose a setup option, as follows.

   Quick setup

   Select this option for basic configuration.

   Advanced setup

   Select this option for custom configuration. Ensure that you create an index for at least the Region where your Active Directory resides.
4. Select a Region for the **Aggregator index Region**.
5. Choose **Turn on Resource Explorer** to save your settings.
6. In the navigation pane, select **Views**, then choose **Create view**.

   > **Note**
   >
   > To show the navigation pane if it's hidden, choose the menu icon (three horizontal bars).

7. a. In the **Create view** page, enter **`license-manager-user-subscriptions-view`** in the **Name**.

   b. Verify that the **Resources filter** is set to **Include all resources**.

   c. In the **Additional resource attributes** section, verify that the **Tags** checkbox is selected.
8. Choose **Create view** to finish.

For more information about creating an AWS Managed Microsoft AD directory, see AWS Managed Microsoft AD prerequisites and Create your AWS Managed Microsoft AD directory in the *AWS Directory Service User Guide*.

To associate users with AWS Managed Microsoft AD, you must provision users in your AWS Managed Microsoft AD directory. For more information, see Manage users and groups in AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.

Security groups

Security groups control the network traffic that's allowed into and out of the resources on your network. To ensure that resources in your user-based subscription environment can communicate, your security groups must meet the following criteria.

Security group for VPC endpoints

Identify or create a security group that permits **inbound** TCP port 1688 connectivity. When you configure your VPC settings, you'll specify this security group. For more information, see Work with security groups.

License Manager associates this security group to the VPC endpoints it creates on your behalf while configuring the VPC. For more information about VPC endpoints, see Access an AWS service using an interface VPC endpoint in the *AWS PrivateLink Guide*.

Security group for Active Directory domain controllers

Ensure that the security group that you use for your AD domain controllers allows outbound traffic to each domain controller's network interface IPv4 address.

Security group for user-based subscription instances

Identify or create a security group that permits the following access to and from your instance. For more information, see Work with security groups.

- **Inbound** TCP port 3389 connectivity from your approved connection sources.
- **Outbound** TCP port 1688 connectivity to reach the VPC endpoints, and to communicate with AWS Systems Manager.

Network configuration

License Manager creates two network interfaces which use the default security group of the VPC where your AWS Managed Microsoft AD is provisioned. These interfaces are used for the service to interact with your directory. For more information, see Step 2: Register your Active Directory in License Manager and What gets created in the *AWS Directory Service Administration Guide*.

After the provisioning process is complete, you can associate a different security group to the interfaces created by License Manager.

DNS resolution

The Active Directory that you've registered for user-based subscriptions must be accessible from any VPCs and subnets that you've configured in License Manager settings. To ensure that Active Directory nodes are accessible, configure DNS resolution as follows:

- Configure DNS forwarding between the VPCs and Active Directories that are configured in your License Manager settings for user-based subscriptions.You can use Amazon Route 53 or another DNS service for DNS forwarding. For more information, see the blog post Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolvers.
- Enable **DNS hostnames** and **DNS resolution** for your VPC. For more information, see View and update DNS attributes for your VPC.

Instances that provide user-based subscription products

For your user-based subscription instances to function as expected, you must meet the following prerequisites:

- Set up a security group for your instances as described in Security groups.
- Ensure that the instances launched to provide user-based subscriptions with Microsoft Office have a route to the subnet where the VPC endpoints are provisioned.
- Instances that provide user-based subscriptions must be managed by AWS Systems Manager in order to have a healthy status. Additionally, your instances must be able to activate their user-based subscription licensing to remain in compliance after license activation.

> **Note**
>
> License Manager will attempt to recover unhealthy instances, but instances that are not able to be return to a healthy status will be terminated. For troubleshooting information

on keeping your instances managed by Systems Manager, and instance compliance, see the Troubleshoot user-based subscriptions in License Manager section of this guide.

- You must have an instance profile role attached to instances providing the user-based subscription products that allows for the resource to be managed by AWS Systems Manager. For more information, see Create an IAM instance profile for Systems Manager in the *AWS Systems Manager User Guide*.
- You must Disassociate users from an instance prior to terminating the instance.

Microsoft Remote Desktop Services

The Microsoft Remote Desktop Services license server requires an administrative user that's defined in the associated Active Directory. That user must be able to perform the following tasks:

- Create an OU under the Active Directory domain
- Domain join instances (create Computer) inside of the OU that is created
- Add a computer object to a Terminal servers group within the Active Directory domain
- Have delegated control for user objects in the Active Directory domain to read and write Terminal Server license server, in order to generate license server reports.

To learn more about delegation, see Delegation of Control in Active Directory Domain Services.

Administrative credentials secret

License Manager uses AWS Secrets Manager to manage the credentials needed for user administration tasks on the Microsoft Remote Desktop Services license server. Before you can set up the license server, you must create a secret in Secrets Manager that contains the credentials for the user who performs user administration tasks on the license server. When you configure the license server settings, you must provide the ID of the secret that you created.

Note

This must be the same user that you've defined for RDS license server report generation.

To create a secret, follow detailed instructions on the Create an AWS Secrets Manager secret page in the *Secrets Manager User Guide*, with the following settings that are specific to License Manager.

> **Important**
>
> To use the secret, License Manager depends on the exact key names, the username value, and the encryption key that are specified in the following list. The secret name must begin with the following prefix: `license-manager-user-`.

On the **Choose secret type** page:

- **Secret type** – Choose **Other type of secret**.
- **Key/value pairs** – Specify the following key pairs to store in the secret.

  Username

  - Key: `username`
  - Value: `Administrator`

  Password

  - Key: `password`
  - Value: *`The password`*
- **Encryption key** – To specify a KMS key other than the `aws/secretsmanager` key, you must attach a policy to the role that you use for accessing License Manager operations. For more information, see IAM roles and permissions.

On the **Configure secret** page:

- **Secret name** – Specify a name for your secret that begins with the prefix that License Manager uses to identify license server credential secrets. For example:

```
license-manager-user-admin-credentials
```

These instructions assume that you are using the AWS Management Console to create your secret. The Secrets Manager User Guide also includes detailed instructions for other methods. For more information about Secrets Manager, see What Is Secrets Manager. For information specifically related to costs, see Pricing for AWS Secrets Manager in the *Secrets Manager User Guide*.

Supported software products for user-based subscriptions in License Manager

AWS License Manager supports user-based subscriptions for Microsoft Visual Studio, and Microsoft Office. Supported software utilization is tracked by License Manager. A single subscription to Windows Server Remote Desktop Services Subscriber Access License (RDS SAL) is required for each user to access a license-included instance that provides a user-based subscription product. For more information, see Get started with user-based subscriptions in License Manager.

Supported Windows operating system (OS) platforms

You can find Windows AMIs that include products covered by the RDS SAL license for the following Windows OS platforms:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Supported software for user-based subscriptions

License Manager supports user-based licensing with the following software.

- Microsoft Visual Studio
- Microsoft Office

Microsoft Visual Studio

Microsoft Visual Studio is an integrated development environment (IDE) that enables developers to create, edit, debug, and publish applications. The provided Microsoft Visual Studio AMIs include the AWS Toolkit for .NET Refactoring and the AWS Toolkit for Visual Studio.

Supported editions

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

The following table details the software subscription names and their associated product value used for License Manager user-based subscription API operations.

Software subscription name	Product value
Visual Studio Enterprise 2022	`VISUAL_STUDIO_ENTERPRISE`
Visual Studio Professional 2022	`VISUAL_STUDIO_PROFESSIONAL`

Microsoft Office

Microsoft Office is a collection of software developed by Microsoft for various productivity use cases including working with documents, spreadsheets, and slide show presentations.

Supported editions

- Office LTSC Professional Plus 2021

The following table details the software subscription names and their associated product value used for License Manager user-based subscription API operations.

Software subscription name	Product value
Office LTSC Professional Plus 2021	`OFFICE_PROFESSIONAL_PLUS`

Active Directory

License Manager supports user-based subscriptions for Microsoft Visual Studio, Microsoft Office, and Remote Desktop Services Subscriber Access License (RDS SAL). Products may support either AWS Managed Microsoft AD or a self-managed active directory that is either deployed within your AWS environment or has network connectivity to a VPC in your AWS environment.

This table indicates which types of Active Directory are supported by each software product when used with user-based subscriptions:.

Software product	AWS Managed Microsoft AD	Self-managed AD
Microsoft Visual Studio	Supported	Not supported
Microsoft Office	Supported	Not supported
RDS SAL Product	Supported	Supported

Additional software

You can install additional software on your instances that aren't available as user-based subscriptions. Additional software installations aren't tracked by License Manager. These installations must be performed using the administrative account for your Active Directory. If you use an AWS Managed Microsoft AD, the administrative account (Admin) is created by default in your directory. For more information, see Admin account in the *AWS Directory Service Administration Guide*.

To install additional software with the Active Directory administrative account, you must:

- Subscribe the administrative account to the product provided by the instance.
- Associate the administrative account to the instance.
- Connect to the instance using the administrative account to perform the installation.

For more information, see Get started with user-based subscriptions in License Manager.

Get started with user-based subscriptions in License Manager

The following steps detail how you can get started with using user-based subscriptions. These steps assume you have already implemented the required prerequisites. For more information, see the Prerequisites to create user-based subscriptions in License Manager.

Steps

- Step 1: Subscribe to a product
- Step 2: Register your Active Directory in License Manager
- Step 3: Configure RDS license server
- Step 4: Launch an instance to provide user-based subscriptions

- Step 5: Associate users to a user-based subscription instance

Step 1: Subscribe to a product

Microsoft products like Office or Visual Studio require an active subscription before you can associate Active Directory users to an instance that includes those products. Subscription products that display a **Subscribe in AWS Marketplace** button in the **Marketplace Subscription Status** column are not subscribed yet.

When you subscribe to a Microsoft user-based subscription product from the AWS Marketplace, License Manager automatically adds a subscription to Microsoft Remote Desktop Services (RDS) for your account, if you don't already have one. RDS is required in order to remotely access the graphical desktops and subscription based Windows applications on EC2 instances launched from license-included AMIs.

You can subscribe to your products directly on the AWS Marketplace using the following links:

- Visual Studio Professional
- Visual Studio Enterprise
- Office LTSC Professional Plus 2021
- Win Remote Desktop Services SAL

Discover and subscribe to products from the License Manager console

You can also discover the required products to subscribe to from the License Manager console.

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **Products**.
3. Choose a product's name or choose the **Subscribe in AWS Marketplace** button to display subscription details.
4. For each of the listed Marketplace products, select **View subscription options**. Review the terms and choose **Subscribe** to proceed.

If you accept the terms, the product subscription will need to be processed. The subscription will have an in progress message until it completes. You can repeat these steps for any other configured products you require. Once all of the required products have an active subscription, you can proceed with registering your Active Directory with the product.

> **Note**
>
> Your estimated bill for charges on the number of users and related costs takes 48 hours to appear for billing periods that haven't closed (marked as **Pending** billing status) in AWS Billing. For more information, see Viewing your monthly charges in the *AWS Billing User Guide*.

Step 2: Register your Active Directory in License Manager

License Manager requires that subscription users are defined in Active Directory in order to associate the users with user-based subscriptions. This can be either an AWS Managed Microsoft AD or a self-managed Active Directory, depending on your subscriptions.

- If you subscribe only to stand-alone Microsoft Office or Visual Studio products, you must configure an AWS Managed Microsoft AD.
- If you subscribe to Win Remote Desktop Services SAL, then you can use either an AWS Managed Microsoft AD or a self-managed Active Directory.

To use Microsoft Office with user-based subscriptions, you must grant License Manager permission to update your VPC configuration. When you configure your VPC, License Manager creates VPC endpoints on your behalf. These endpoints are required for your resources to connect to activation servers and remain in compliance.

You must configure DNS forwarding for any additional VPCs that you register for user-based subscriptions. If you have user-based subscriptions in multiple AWS Regions, each Region must have its own Active Directory with DNS forwarding configured.

> **Important**
>
> You must allow License Manager to create the required service-linked role before you can proceed. For more information, see the Prerequisites to create user-based subscriptions in License Manager.

Registration steps differ in the console, depending on which products you've subscribed to. If you've subscribed to `Win Remote Desktop Services SAL`, select the **Microsoft RDS SAL** tab.

If you subscribe to Microsoft Office or Visual Studio and do NOT subscribe to RDS SAL, select the **Stand-alone MSO subscriptions** tab.

Microsoft RDS SAL

Register AWS Managed Microsoft AD

To register AWS Managed Microsoft AD as your Active Directory for user-based subscriptions, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Navigate to **User-based subscriptions** under **Settings** in the left navigation pane.
3. In the **Remote Desktop Services (RDS)** tab on the **User based subscriptions** page, choose **Register Active Directory**.
4. Select the **AWS Managed Active Directory** option to enter details.
5. Select your managed directory from the **AWS Active Directory** list, or create a new managed directory and then come back and select it.
6. Choose **Register** to register your AWS Managed Active Directory.

Register self-managed Active Directory

To register a self-managed Active Directory for user-based subscriptions, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Navigate to **User-based subscriptions** under **Settings** in the left navigation pane.
3. In the **Remote Desktop Services (RDS)** tab on the **User based subscriptions** page, choose **Register Active Directory**.
4. Select the **Self-managed Active Directory** option to enter details.
5. Enter the **Active Directory domain**, along with primary and secondary private IPv4 addresses for your directory.
6. In the **Networking** section, select the **VPC** and two **Subnets** where your Active Directory resides.
7. Select the administrative credentials **Secret** that you created as part of the prerequisites for your Microsoft RDS subscription.

Stand-alone MSO subscriptions

Register AWS Managed Microsoft AD

To register AWS Managed Microsoft AD as your Active Directory for user-based Microsoft Office and Visual Studio subscriptions, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Navigate to **User-based subscriptions** under **Settings** in the left navigation pane.
3. On the **User based subscriptions** page, select the tab for the Microsoft Office or Visual Studio subscription product that you want to register, and then choose **Register Active Directory**.
4. Select your managed directory from the **AWS Active Directory** list, or create a new managed directory and then come back and select it.
5. Choose **Register** to register your AWS Managed Active Directory.

When you register your Active Directory, License Manager creates two network interfaces so that the service can communicate with your directory. The network interface will have a description similar to *AWS created network interface for LicenseManager <directory_id>*.

Active Directory registration from the AWS CLI

You can register your Active Directory as the identity provider for user-based subscriptions with the RegisterIdentityProvider operation.

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product-name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}"
```

Configure Active Directory and your VPC for user-based subscriptions (AWS CLI)

You can register your Active Directory as the identity provider and configure your VPC for user-based subscriptions with the RegisterIdentityProvider operation.

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product_name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}" --settings
 "Subnets=[subnet-1234567890abcdef0,subnet-021345abcdef6789],SecurityGroupId=sg-1234567890abcde
```

For more information about the available software products, see Supported software products for user-based subscriptions in License Manager.

Step 3: Configure RDS license server

The Microsoft Remote Desktop Services (RDS) license server issues Subscriber Access Licenses (SALs) to Active Directory users when they access EC2 instances that provide user-based subscription Microsoft products. After you've completed steps 1 and 2, you can configure your license server, as follows.

Ensure that you've completed the User-based subscription prerequisites for RDS before you begin. This process assumes that you have already set up your Active Directory.

Configure RDS license server for user-based subscriptions (Console)

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Navigate to the **User-based subscriptions** page, under **Settings** in the left navigation pane.
3. On the **Remote Desktop Services (RDS)** tab, you should see one or more Active Directories in the list. There may be a prompt displayed to let you know that you need to configure RDS for your Active Directory.
4. From the prompt or from the **Actions** menu, choose **Configure RDS License Server**.
5. In the **Configure RDS License Server** dialog, You can configure the following settings:

   Active Directory

   This section has key details for the directory that's connected to the RDS license server that you configure.

   Secret

   You must choose an existing secret or create a new one for the credentials that are used for user administration tasks on the license server. The first part of the secret name must follow the pattern that's described in Administrative credentials secret section of the User-based subscription prerequisites.

   Tags

   You can optionally enter tags for your license server resource.
6. Choose **Configure** to save your settings.

Step 4: Launch an instance to provide user-based subscriptions

After you have subscribed to a product, you must launch instances for your users to connect to from the AWS Marketplace AMI that includes the product. After you launch an instance, AWS Systems Manager attempts to join the instance to the Active Directory domain and perform additional configuration and hardening on the resource. The configurations to make the instance ready to use can take around 20 minutes to complete. You can confirm the resource is ready to use from the **User association** page of the License Manager console by checking for a **Health status** of **Active** for the instance.

To launch an instance with user-based subscriptions, see Launch an instance from a license included AMI.

Step 5: Associate users to a user-based subscription instance

Once you have subscribed to the required product's AWS Marketplace AMI, you can subscribe users to a product and associate them to an instance that provides the product. You can subscribe users to products and associate them with an instance in a single step, or separately. When you subscribe a user, the directory is checked to ensure that the user identity is present. One subscription is created for each user you subscribe to the product.

Each user must have a subscription to both Windows Server Remote Desktop Services Subscriber Access License (RDS SAL) and the product they will use.

When your account has subscribed to RDS SAL as detailed in Step 1: Subscribe to a product, License Manager automatically subscribes the users in your Active Directory to RDS SAL when they subscribe to a user-based subscription product.

> **Note**
>
> If a user who has never subscribed logs into an instance that is associated with RDS SAL, License Manager automatically subscribes them and begins Microsoft RDS billing. Billing continues until they are unsubscribed and their license token that was issued by the RDS SAL license server expires.
>
> Similarly, if a previously subscribed user unsubscribes, but continues to log in after their RDS SAL license token expires, they are automatically re-subscribed, and billing continues until they are again unsubscribed and their token expires.

For more information about subscription charges and billing, see Subscription charges in License Manager.

The **Products** page in License Manager displays active subscriptions by listing their **Marketplace subscription status** as **Active**. In the product details page, License Manager displays active user subscriptions with a **Status** of **Subscribed**.

> **Important**
>
> If your Active Directory is not configured with the product, a notification bar appears at the top of the console advising you to adjust the directory settings. On the notification bar, choose **Open settings** to access the **Settings** page in License Manager and edit your directory.
> Each user must have a subscription to both RDS SAL and the product they will use. Subscribing users to a product in which the **Marketplace subscription status** is **Inactive** will fail.

Subscribe users to a product and associate them to an instance

When you select an instance to associate users to, you can optionally subscribe them to the products that the instance provides if they're not already subscribed. Use one of the following methods to subscribe and associate users.

Console

To associate users to an instance, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **User association**.
3. Select the instance that you want to associate users with, then choose one of the following options:

   Associate users

   Specify up to 20 user names that exist in your directory, including the **Domain name** if they exist in a trusted domain, and choose **Associate**. *If you use this method, users must already be subscribed to the products that the instance provides.*

Subscribe & Associate users

Specify up to 20 user names that exist in your directory, including the **Domain name** if they exist in a trusted domain, and choose **Subscribe & Associate**.

(Optional) Review user associations

On the **User association** page, the users you selected are displayed under **Users** with an **Association Status** of **Associated**.

(Optional) Review subscribed users

On the **Products** page, choose the **Product name**. Subscribed users are displayed under **Users** with a **Status** of **Subscribed**.

AWS CLI

You can associate users with an instance launched to provide the user-based subscription with the AssociateUser operation.

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}"
```

To associate self-managed Active Directory users to an instance (AWS CLI)

You can associate users from your self-managed Active Directory with an instance launched to provide the user-based subscription with the AssociateUser operation.

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}" --domain <self-managed-domain-name>
```

For more information about the available software products, see Supported software products for user-based subscriptions in License Manager.

Subscribe users to a product

You can subscribe users to a product using one of the following methods.

Console

Subscribe users to a product (Console)

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **Products**.
3. Select a product to subscribe users to in which the **Marketplace subscription status** is **Active**.
4. If the product is Microsoft RDS, select the registered Active Directory that contains the users to subscribe.
5. Choose **Subscribe user** to continue.
6. Specify up to 20 user names that exist in your directory, including the **Domain name** if they exist in a trusted domain, and choose **Subscribe**.

   Users that have a subscription are displayed under **Users** with a **Status** of **Subscribed**.

AWS CLI

Subscribe users to a product (AWS CLI)

You can subscribe users to a product that is registered with your identity provider using the StartProductSubscription operation.

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 ""ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}"
```

Subscribe users to a product with a self-managed Active Directory (AWS CLI)

You can subscribe users from your self-managed Active Directory to a product that is registered with your AWS Managed Microsoft AD directory using the StartProductSubscription operation.

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 'ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}' --
domain <self-managed-domain-name>
```

For more information about the available software products, see Supported software products for user-based subscriptions in License Manager.

Users that have a subscription will be displayed under **Users** with a **Status** of **Subscribed**.

Configure Active Directory GPO for more active remote user sessions

By default, Microsoft RDS allows a maximum of two user sessions at the same time on an EC2 Windows instance that provides user-based subscription products. After you've configured your License Server endpoints, you can configure Microsoft RDS to allow more than two user sessions at the same time with an Active Directory Group Policy Object (GPO), as follows.

Prerequisite

You must have created a license server in your environment. To create a license server, see Step 3: Configure RDS license server.

1. The tool that you use to configure your GPO depends on where you run it from, as follows:

   Central configuration from your domain controller

   Log into your Active Directory domain controller as an administrator, and open the Windows Group Policy Management Console.

   Configure group policy on the session host

   Log into your License Server as an administrator, and open the Local Group Policy Editor.
2. From the management console or policy editor, edit the group policy to specify the session hosts that connect through Microsoft RDS. You can find the endpoint for your RDS License Server in the License Manager product details page, or with the list-license-server-endpoints command in the AWS CLI.
3. Set the licensing mode for the Remote Desktop Session Host to `Per User`, and save.

For more information about configuring your RDS License Server for License Manager, see the section called “Step 3: Configure RDS” in the Get started topic. For more information about configuration for Microsoft RDS session hosts, see License Remote Desktop session hosts.

Launch an instance from a license included AMI

After you have subscribed to a product, you must launch instances for your users to connect to from the AWS Marketplace AMI that includes the product. After you launch an instance, AWS Systems Manager attempts to join the instance to the Active Directory domain and perform additional configuration and hardening on the resource. The configurations to make the instance ready to use can take around 20 minutes to complete. You can confirm the resource is ready to use from the **User association** page of the License Manager console by checking for a **Health status** of **Active** for the instance.

> **Important**
>
> The instances you launch must meet the required prerequisites to be in compliance. Resources that are unable to complete the initial configuration are terminated. For more information, see the Prerequisites to create user-based subscriptions in License Manager and Troubleshoot user-based subscriptions in License Manager.

Launch an instance with user-based subscriptions

1. Access the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Under **Images**, choose **AMI Catalog**.
3. Choose **AWS Marketplace AMIs**.
4. Enter the product name into the search box and press enter. For example, you might search for **`Visual Studio`**.
5. Under **Publisher**, select **Amazon Web Services**.
6. Choose **Select** for the product that you want to launch an instance to provide user-based subscriptions.
7. Choose **Continue** to proceed.
8. Choose **Launch Instance with AMI**.
9. Complete the wizard while ensuring that you:
    a. Choose a Nitro based instance type that is not Graviton based.
    b. Choose a VPC and subnet from which your instance can connect to your AWS Managed Microsoft AD directory.

c. Choose a security group that permits connectivity from your instance to your Active Directory.

d. Expand **Advanced details** and choose an IAM role that allows Systems Manager functionality for your instance.

10. Choose **Launch instance**.

When you have running instances from the AWS Marketplace AMI, you must subscribe users to the product and associate them with instances, which provide the product so that they can use it.

Launch an instance from a specific operating system version AMI

When you launch an instance from an AMI that supports `Office LTSC Professional Plus` or Microsoft Visual Studio, the launch defaults to the latest Windows operating system version of the AMI (for example Windows Server 2025). To launch with a specific operating system version AMI, follow these steps.

1. Open the AWS Marketplace console at https://console.aws.amazon.com/marketplace.
2. Choose **Manage subscriptions** from the navigation pane.
3. To streamline subscription results, you can search for all or part of the subscription name. For example, `Office LTSC Professional Plus 2021` or `Visual Studio Enterprise`.
4. Select **Launch new instance** from the subscription panel. This opens a launch configuration page.
5. To launch an instance from an AMI that's based on an earlier version of the Windows OS platform, select the **full AWS Marketplace website** link, located under the **Software version**. This takes you to a configuration page where you can select from a list of versions.
6. The list shows the latest AMI versions for the supported Windows OS platforms. Select the Windows OS version that you want to launch from.

Connect to a user-based subscription instance with RDP

Once you have associated users with the instance providing the product, they can connect to the instance if the **Health status** of the instance is **Active**. The users will need to connect with their user credentials for the domain to use the product with their associated identity.

> **Important**
>
> The process of creating the EC2 instance and preparing it for users can take around 20 minutes. The **Association status** of the instance must be **Active** in order to access it and use the product.

To connect to instances with a user-based subscription

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **User association**.
3. On the **User association** page, confirm the instance's **Health status** is **Active**.
4. Make note of the instance ID as you will need it to gather connection details.
5. Follow the steps listed in Connect to your Windows instance using RDP while ensuring to specify the fully qualified user name of the associated user.

Modify firewall settings for your Microsoft Office subscription

A firewall protects your network resources from unauthorized inbound or outbound traffic. The rules that you define for your security group act as the firewall for the VPC resources that work together to provide user-based subscriptions Microsoft Office on EC2 Windows instances.

You can use the following steps to edit the subnets and security group. License Manager uses your settings to provision endpoints for Microsoft Office with AWS PrivateLink. For more information about VPC endpoints, see What is AWS PrivateLink? in the *Amazon Virtual Private Cloud* documentation.

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. Navigate to the **User-based subscriptions** page, under **Settings** in the left navigation pane.
3. To edit firewall settings, select the Microsoft Office subscription product tab, and then choose **Edit** from the top of the **Firewall** section. This opens the **Edit Firewall** dialog.
4. After you change your settings, choose **Save** to update, or **Cancel** to keep your current settings.

It might take a few minutes for License Manager to complete changes for these settings.

Manage subscription users for License Manager user-based subscriptions

To ensure the accuracy of billing and reporting for Microsoft Office and Visual Studio product subscriptions in License Manager, and to prevent unauthorized access to subscription resources, you can manage user access as follows.

Disassociate users from an instance

Disassociate a user from an instance that hosts a License Manager user-based Microsoft Office or Visual Studio product subscription to remove access to the resource.

Unsubscribe users

Unsubscribe users from user-based Microsoft Office or Visual Studio product subscriptions in AWS License Manager to stop incurring subscription charges for those individuals.

Note

Deleting a user from Active Directory will not alter user associations or subscriptions for Microsoft Office and Visual Studio products. You must disassociate the user in License Manager from the subscription product details page to remove their association with an instance. Then you must unsubscribe the user.
This topic does not cover Active Directory administration.

Contents

- Disassociate users from an instance that provides License Manager user-based subscriptions
- Unsubscribe users from user-based product subscriptions in License Manager

Disassociate users from an instance that provides License Manager user-based subscriptions

To remove user access to an instance that provides License Manager user-based subscriptions, you can disassociate the subscribed user from that instance. This change does not affect the user's subscription status. To unsubscribe a user and stop subscription charges for that individual, see Unsubscribe users from user-based product subscriptions in License Manager.

Disassociate subscription users from an instance

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **User association**.
3. Select the instance that you want to disassociate users from.
4. Select the user names to disassociate, then choose **Disassociate users**.

Unsubscribe users from user-based product subscriptions in License Manager

You must unsubscribe a user from a Microsoft Office or Visual Studio user-based subscription product to stop incurring charges for them. Microsoft RDS is billed on a per user, per month basis based on a combination of the user subscription and the client access license (CAL) token that's issued from the license server when the user connects to an instance that provides the subscription product. For more information, see Microsoft RDS billing in License Manager.

> **Important**
>
> For Microsoft Office or Visual Studio user-based subscription products, you must first disassociate the Active Directory user from all instances where they are currently associated before you can unsubscribe them.

Unsubscribe users from user-based product subscriptions

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under **User-based subscriptions**, choose **Products**.
3. Select the product that you want to unsubscribe users from.
4. Select the user names to unsubscribe, then choose **Unsubscribe users**.

Deregister an Active Directory from License Manager settings

You can deregister your Active Directory from License Manager settings if you no longer want to use it for user-based subscriptions. Deregistering the directory configuration from License Manager settings doesn't delete the directory. When you deregister the directory from the settings, you can no longer associate users from that directory for user-based subscriptions in License Manager.

Prerequisites

Before you deregister the directory from License Manager settings, you must perform the following tasks:

1. Disassociate users from an instance from each instance that references the directory that you want to deregister.
2. After all of the subscription users are disassociated from the instance, terminate the instance. Repeat until all instances that refer to the Active Directory are terminated.
3. You also need to Unsubscribe users that belong to the Active Directory you will deregister to stop incurring changes for them.

Deregister

> **Important**
>
> If your Active Directory is used for Microsoft RDS SAL users, you must delete the associated license server endpoint before you deregister and delete the AD.

Deregister the Active Directory from License Manager settings

After you've completed all of the prerequisite tasks, open the License Manager console at https://console.aws.amazon.com/license-manager/.

1. In the left navigation pane, choose **Settings**.
2. On the **Settings** page, under the AWS Managed Microsoft AD section, choose **Remove**.
3. Enter the required text to confirm that you want to remove the directory and choose **Remove**.

After you choose **Remove**, the **AWS Managed Microsoft AD** section on the **Settings** page displays your **Directory ID** with the **Status** of **Configuring**. Once the configuration process is complete, the directory is removed from the **AWS Managed Microsoft AD** section.

Troubleshoot user-based subscriptions in License Manager

The following are troubleshooting tips to help solve issues that can occur with user-based subscriptions in AWS License Manager.

Contents

- Troubleshoot instance compliance
- Troubleshoot license compliance
- Troubleshoot instance connectivity
- Troubleshoot failures to join the domain
- Troubleshoot Systems Manager connectivity
- Troubleshoot Systems Manager Run Command
- Troubleshoot Microsoft RDS Licensing failures
- Troubleshoot Microsoft Office activation failures

Troubleshoot instance compliance

Instances providing user-based subscriptions must remain in a healthy status to be in compliance. Instances that are marked as unhealthy no longer meet the required prerequisites. License Manager will attempt to return the instance to a healthy status, but instances that are not able to return to a healthy status are terminated.

Instances which are launched to provide user-based subscriptions and are unable to complete the initial configuration will be terminated. You must correct the configuration issue and launch new instances to provide user-based subscriptions in this scenario. For more information, see the Prerequisites to create user-based subscriptions in License Manager.

Troubleshoot license compliance

If you configured your Active Directory to provide user-based subscriptions with Microsoft Office, you must ensure your resources can connect to the VPC endpoints License Manager creates. The endpoints require inbound traffic on TCP port 1688 from the instances providing user-based subscriptions.

You can use Reachability Analyzer to help confirm that the networking configuration from your instances providing user-based subscriptions and the VPC endpoints are configured properly. You can specify an instance ID launched in a subnet providing user-based subscriptions as the source, and a VPC endpoint provisioned for Microsoft Office products as the destination. Specify TCP as the protocol and 1688 for the destination port for the path to analyze. For more information, see How can I troubleshoot connectivity issues over my gateway and interface VPC endpoints?.

Troubleshoot instance connectivity

Users must be able to use RDP to connect to the instances providing user-based subscriptions in order to use the products within. For more information on troubleshooting instance connectivity, see Troubleshoot connecting to your Windows instance in the *Amazon EC2 User Guide*.

Troubleshoot failures to join the domain

Users must be able to connect to the instances providing the user-based subscription products with their user identities from the Active Directory configured in the License Manager settings. Instances that fail to join the domain will be terminated.

To troubleshoot, you may need to launch an instance and manually join the domain so that the resource is not terminated before you can investigate. The instance must receive and execute the Systems Manager Run Command successfully, and the instance must also be able to complete the domain join within the operating system. For more information, see Understanding command statuses in the *AWS Systems Manager User Guide* and How to troubleshoot errors that occur when you join Windows-based computers to a domain on the Microsoft website.

If you launch instances from a custom AMI that uses a user-based subscription product AMI as its base image, you must perform Sysprep steps on the custom AMI to ensure a unique computer name at launch. Before you run Sysprep with /generalize, ensure that the machine is removed from the domain.

Troubleshoot Systems Manager connectivity

Instances that provide user-based subscriptions must be managed by AWS Systems Manager or they will be terminated. For more information, see Troubleshooting SSM Agent and Troubleshooting managed node availability in the *AWS Systems Manager User Guide*.

Troubleshoot Systems Manager Run Command

Run Command, a capability of Systems Manager, is used with instances providing user-based subscriptions to join the domain, harden the operating system, and perform access audits for the included product. For more information, see Understanding command statuses in the *AWS Systems Manager User Guide*.

Troubleshoot Microsoft RDS Licensing failures

If you experience issues with CAL (Client Access License) issuance, check whether there are additional Microsoft RDS licensing servers present in your server farm or Terminal Servers group.

We do not recommend having additional licensing servers in these locations, as that can interfere with CAL issuance and lead to licensing complications.

To resolve this issue, ensure that only the intended Microsoft RDS servers remain in your server farm and Terminal Servers group.

When troubleshooting licensing issues, be aware that connections using the /admin flag bypass standard licensing checks, as this flag is intended for administrative purposes, and doesn't consume a CAL. This can mask underlying licensing problems. To diagnose licensing issues, verify that standard user connections (without the /admin flag) are functioning correctly for license management.

Troubleshoot Microsoft Office activation failures

If Microsoft Office activation fails, verify that your instance has access to the VPC that's defined for License Manager. Either of the following options satisfies this requirement:

- Your instance is running in the VPC that's onboarded with License Manager (through VPC endpoint)
- Your instance is running in a VPC that's peered with the License Manager onboarded VPC.

To resolve this issue, ensure that your instance is moved to the correct VPC, or establish VPC peering with the License Manager onboarded VPC.

Manage Linux subscriptions in License Manager

With AWS License Manager, you can view and manage commercial Linux subscriptions that your Amazon EC2 instances use. You can track utilization of your Linux subscriptions for the AWS Regions and accounts in AWS Organizations that you've defined in your settings. License Manager gives you a comprehensive view of your running instances that use Linux subscriptions. It also indicates when an instance has more than one subscription defined.

The data that License Manager discovers is aggregated and displayed in the License Manager console and in the Amazon CloudWatch dashboard. You can also access your subscription data through the AWS CLI and the License Manager Linux subscription API or associated SDKs.

Linux license subscriptions can come from the following sources:

Subscription-included AMIs

- Red Hat Enterprise Linux (RHEL)
- RHEL Bring Your Own Subscription model (BYOS) with the Red Hat Cloud Access Program
- SUSE Linux Enterprise Server
- Ubuntu Pro subscription-included AMI

Third-party subscription providers

- RHEL subscription from Red Hat Subscription Manager (RHSM)

Linux subscription discovery uses the eventual consistency model. A consistency model determines the manner and timing in which data is loaded and presented in your Linux subscriptions view. With this model, License Manager ensures that your Linux subscription data is updated periodically from your resources. In the event that some data is not ingested during these intervals, the information is delivered at the next metric emission. This behavior can delay resources, such as newly launched EC2 commercial Linux instances, from displaying in the Linux subscriptions dashboard.

> **Note**
>
> It can take up to 36 hours for the initial resource discovery to complete, and up to 12 hours for newly launched instances to be discovered and reported. Once your resources are discovered, Amazon CloudWatch metrics are emitted hourly for Linux subscriptions data.

If your accounts are in AWS Organizations, you can register a member account as the delegated administrator. For more information, see Delegated administrator settings in License Manager.

Duplicate subscriptions detected

When License Manager detects two Linux subscriptions on the same EC2 instance, it sets the duplicate subscription alert. You can view and filter Linux subscription data from the **Instances** page in the License Manager console.

Red Hat Enterprise Linux 7 Extended Lifecycle Support (RHEL 7 ELS) instances: When you launch an instance from a subscription-included AMI for RHEL 7 ELS, you should still register your instance

with Red Hat and consume an entitlement. In this case, License Manager reports a duplicate subscription, but that's the expected behavior.

Other Red Hat Linux instances: We recommend that you search the subscription inventory in the Red Hat Hybrid Cloud Console to find out which subscriptions your instance consumes.

Additional topics

- Configure Linux subscription discovery in License Manager
- View discovered instance data in License Manager
- Billing information for Linux subscriptions in License Manager
- Manage Amazon CloudWatch alarms for Linux subscriptions in License Manager

Configure Linux subscription discovery in License Manager

You can configure discovery of Linux subscriptions through the License Manager console, the AWS CLI, the License Manager Linux subscription API, or the associated SDKs. When you activate discovery of Linux subscriptions for the AWS Regions you specify, you can optionally extend discovery to your accounts in AWS Organizations. If you no longer want to track subscription utilization, you can also deactivate discovery.

> **Note**
>
> You can discover and display up to 5,000 resources per account per AWS Region by default. To request an increase to these limits, use the limit increase form.

Topics

- Configure Linux subscription discovery
- Activate Red Hat Subscription Manager subscription discovery
- Resource discovery status reasons
- Deactivate discovery of Linux subscriptions

Configure Linux subscription discovery

To configure Linux subscription discovery from the **Settings** page in the License Manager console, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Settings**. This opens the **Settings** page.
3. Open the **Linux subscriptions** tab, and choose **Configure**. This opens the **Configure Linux subscriptions settings** panel.
4. Select the **Source AWS Regions** where Linux subscription discovery should run.
5. To aggregate subscription data across your accounts in AWS Organizations, select **Link AWS Organizations**. This option only appears if AWS Organizations is configured for your account.
6. Review and acknowledge the option that grants AWS License Manager permission to create a service-linked role for Linux subscriptions.
7. Choose **Save configuration**.

Activate Red Hat Subscription Manager subscription discovery

To retrieve subscription information from Red Hat Subscription Manager (RHSM) on your behalf, License Manager must provide your Red Hat customer account API credentials.

Prerequisites

Before you activate subscription discovery, make sure that you've met the following prerequisites.

- Default discovery for Linux subscriptions must be activated for your AWS account before you can configure RHSM subscription discovery. If default discovery is **Not activated**, see Configure Linux subscription discovery.
- If you use a corporate Red Hat login provided by your Organization Administrator, ensure that your login ID has the following roles and permissions assigned:
  - **Role:** Manage your subscriptions
  - **Permissions:** `View All`, or `View/Edit All`

  If your login ID doesn't have the required roles and permissions, contact your Red Hat portal Organization Administrator and request to add them to your login. For more information about Red Hat roles and permissions, see Roles and Permissions for Red Hat Customer Portal. For more information about how to contact your Red Hat Portal Organization Administrator, see How do I know who my Organization Administrator is? in the *Red Hat Customer Portal Knowledgebase*.
- To activate RHSM subscription discovery, you must provide the Red Hat customer account API offline token, or an AWS Secrets Manager secret that contains the offline token. To get your

offline token, follow the steps described in Generating a new offline token on the *Red Hat Documentation* website.

> **Important**
>
> Your security is important to us. Your Red Hat offline access token is stored securely in Secrets Manager. License Manager uses your secret to generate a temporary access token each time it requests subscription details from Red Hat.

Activation

To activate RHSM discovery from the **Settings** page in the License Manager console, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Settings**.
3. On the **Settings** page, open the **Linux subscriptions** tab.
4. Choose **Edit** to update your Linux subscription settings. This opens the **Configure Linux subscriptions discovery** page.
5. To begin the activation process, select the **Activate Red Hat Subscription Manager (RHSM) discovery** check box. This displays the **Link RHSM account** panel.
6. Select the **Secret (Token)** option that applies for your secret, and follow remaining steps that depend on which option you choose.
7. **Option: Create a new secret – *recommended***

   Provide the Red Hat offline access token and let License Manager create the access secret in Secrets Manager on your behalf.

   a. Enter a name for your secret in **Secret name**.
   b. Paste your Red Hat offline access token into the **Offline token** box. Make sure that there are no extra spaces or line breaks before or after your token value. You can generate your Red Hat offline access token on the Red Hat Subscription Manager API Tokens page.

   Option: Select a secret

   Select an existing secret in Secrets Manager that contains your Red Hat offline access token.

8. (optional) Add tags for your secret.
9. Select the check box at the bottom of the page to acknowledge that by activating Red Hat Subscription Manager discovery, you grant access to the AWS License Manager service to collect data that relates to Red Hat subscriptions used on Amazon EC2 instances.
10. Choose **Activate**.

Resource discovery status reasons

AWS License Manager will display a status and a corresponding status reason for each AWS Region you choose to enable discovery for Linux subscriptions. The status reason will vary if you have linked Linux subscriptions with AWS Organizations:

- In progress
- Successful
- Failed

The status reason that displays for each Region you choose will show up to two status reasons at a time. The following table provides more detail:

Status reason action	Description
Account-onboard	Onboarding a single account.
Account-offboard	Offboarding a single account.
Org-onboard	Onboarding an entire organization.
Org-offboard	Offboarding an entire organization.

You can call the `UpdateServiceSettings` API and subsequently call the `GetServiceSettings` API to monitor the progress of enabling Linux subscriptions. Each status and status reason can apply to multiple Regions at once. The follow table provides more detail on the status and status reason:

Status	Status reason	Description
In Progress	`"Region": "Account-Onboard: Pending"`	Enabling Linux subscriptions for a single account is in progress.
	`"Region": "Org-Onboard: Pending"`	Enabling Linux subscriptions for an organization is in progress.
	`"Region": "Account-Offboard: Pending`	Disabling Linux subscriptions for a single account is in progress.
	`"Region": "Org-Offboard: Pending`	Disabling Linux subscriptions for an organization is in progress.
Successful	`"Region": "Account-Onboard: Successful"`	Enabling Linux subscriptions for a single account was successful.
	`"Region": "Org-Onboard: Successful"`	Enabling Linux subscriptions for an organization was successful.
	`"Region": "Account-Offboard: Successful`	Disabling Linux subscriptions for a single account was successful.
	`"Region": "Org-Offboard: Successful`	Disabling Linux subscriptions for an organization was successful.
Failed	`"Region": "Account-Onboard: Failed - Service-linked role not present"`	Enabling Linux subscriptions for a single account has failed due to the required service-linked role not being created. Create the required role, and try again.
	`"Region": "Account-Onboard: Failed - An internal error occurred"`	Enabling Linux subscriptions for a single account has failed due to an internal error.
	`"Region": "Org-Onboard: Failed - Account`	Enabling Linux subscriptions for an organization has failed due to the account performing the

Status	Status reason	Description
	`isn't the management account"`	operation not being the organizat ion's management account. Log in to the management account, and try again.
	`"Region": "Org-Onboard: Failed - Account isn't part of an organiz ation"`	Enabling Linux subscriptions for an organization has failed due to the account performing the operation not being in an organization. Try the operation from an account in the organizat ion, or add this account to the organization, and try again.
	`"Region": "Org-Onboard: Failed - Linux subscript ions can't access the organization"`	Enabling Linux subscriptions for an organization has failed due to License Manager not having permissions to access the organization. Create the service-l inked role for Linux subscriptions , and try again.

Deactivate discovery of Linux subscriptions

You can deactivate discovery of Linux subscriptions from the AWS License Manager settings page. However, if you have activated discovery for

> **Warning**
>
> If you disable discovery, all of your data previously discovered for Linux subscriptions will be removed from AWS License Manager.

To disable discovery for Linux subscriptions

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.

2. In the left navigation pane, choose **Settings**.
3. On the **Settings** page, choose the **Linux subscriptions** tab and choose **Disable Linux subscription discovery**.
4. Enter **`Disable`** and then choose **Disable** to confirm deactivation.
5. (Optional) Remove the service-linked role used for Linux subscriptions. For more information, see Delete a service-linked role for License Manager.
6. (Optional) Disable trusted access between License Manager and your organization. For more information, see AWS License Manager and AWS Organizations.

View discovered instance data in License Manager

After License Manager completes the initial resource discovery process in your selected AWS Regions, you can view the results in the console. If you chose to link AWS Organizations, License Manager aggregates data from accounts across your organization. To view a list of instances with subscriptions that meet your filter criteria, navigate to the **Instances** section of the AWS License Manager console. The list displays the following key fields.

- **Instance ID** – The ID of the instance.
- **Status** – The status of the instance.
- **Instance type** – The type of instance.
- **Subscription** – The name of the license subscription that the instance uses.
- **Duplicates alert** – Indicates that you have two different license subscriptions for the same software on your instance.
- **Account ID** – The ID of the account which owns the instance.
- **Region** – The AWS Region in which the instance resides.
- **AMI ID** – The ID of the AMI used to launch the instance.
- **Usage operation** – The operation of the instance and the billing code that is associated with the AMI. For more information, see Usage operation values.
- **Product code** – The product code associated with the AMI used to launch the instance. For more information, see AMI product codes.
- **LastUpdatedTime** – The time in which the last discovery updated the instance details.

Topics

- View data for all instances
- View data for instances by subscription

View data for all instances

You can view and filter Linux subscription data that License Manager discovered for the instances in your account or AWS Organizations, as follows.

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Instances**. This displays a list of instances with Linux subscription data.
3. (Optional) You can use the following filters to streamline your results:
   - Account
   - AMI ID
   - Duplicate subscription
   - Instance ID
   - Region
   - Product code
   - Usage operation
4. (Optional) Choose **Export view to CSV** to export data for all of your instances as a comma-separated values file (CSV).

View data for instances by subscription

You can view data for all instances has have been aggregated across accounts in your organization within the chosen Regions.

To view discovered data for instances with a specific subscription

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription you would like to view data for.
4. Choose the **Instances** tab and review the data as needed in the console. You can filter the data by:

- Instance ID
- Account
- Region
- AMI ID
- Usage operation
- Product code

5. (Optional) Choose **Export view to CSV** to export data for your instances with this subscription as a comma-separated values file (CSV).

Billing information for Linux subscriptions in License Manager

Each commercial Linux subscription running on Amazon EC2 has billing information associated with the Amazon Machine Image (AMI). Commercial Linux subscriptions have Amazon EC2 usage operation, AWS Marketplace product code, or a combination of both. For more information, see AMI billing information fields in the *Amazon Elastic Compute Cloud User Guide for Linux Instances* and AMI product codes in the *AWS Marketplace Seller Guide*.

Subscription name	Amazon EC2 usage operation	AWS Marketplace product code	Subscription type
Red Hat Enterprise Linux Server BYOS	RunInstances:00g0	✗	Bring Your Own Subscription model (BYOS)
Red Hat Enterprise Linux Server	RunInstances:0010	✗	EC2 subscription-included
Red Hat Enterpris e Linux with High Availability Add-on	RunInstances:1010	✗	EC2 subscription-included
Red Hat Enterpris e Linux with SQL Server Standard and High Availability	RunInstances:1014	✗	EC2 subscription-included

Subscription name	Amazon EC2 usage operation	AWS Marketplace product code	Subscription type
Red Hat Enterprise Linux with SQL Server Enterprise and High Availability	RunInstances:1110	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110	✗	EC2 subscription-included
SUSE Linux Enterprise Server	RunInstances:000g	✗	EC2 subscription-included
Red Hat Enterprise Linux for SAP with High Availability and Update Services	RunInstances:0010	✓	AWS Marketplace subscription [1]
SUSE Linux Enterprise Server with SAP	✗	✓	AWS Marketplace subscription
Ubuntu Pro	RunInstances:0g00	✓	AWS Marketplace subscription
Red Hat Enterprise Linux Workstation	✗	✓	AWS Marketplace subscription

[1] This subscription has both an Amazon EC2 usage operation and AWS Marketplace product code.

Usage metrics for Linux subscriptions

The following metrics and dimensions are available for Linux subscriptions:

Metric	Description
RunningInstancesCount	The total number of instances running in the current account that are grouped by the subscription name, or by subscription name and Region. Units: Count Dimensions: `SubscriptionName` : The name of the subscription. `Region`: The Region where the resource using a commercial Linux subscription was discovered.

Manage Amazon CloudWatch alarms for Linux subscriptions in License Manager

The **Linux subscriptions** list page in the License Manager console shows the following key details, including the Amazon CloudWatch alarms that you have configured for each Linux subscription that License Manager found on your instances.

- Subscription name
- Subscription type
- Number of running instances per subscription
- Configured Amazon CloudWatch alarms

When you choose a Linux subscription from the list page, the **Usage metrics and alarms** tab displays data for that subscription. In this tab, Amazon CloudWatch dashboards display for the chosen subscription within the License Manager console. You can adjust the dashboard to encompass a certain time frame, or *evaluation range,* in hours, days, or a week from a selected date.

In the **Usage metrics and alarms** tab, each subscription has an **Alarms** section with the following details:

- **Alarm name** – The name of the alarm.
- **State** – The state of the alarm.
- **Dimension** – The dimensions of the alarm. The dimension will include the AWS Region and instance type that was defined.
- **Condition** – The condition of the alarm. The condition will include the comparison operator and alarm threshold value that was defined.

You can create CloudWatch alarms using the dimensions and conditions you define to track and alert based on your current subscription utilization. The Linux subscriptions console displays a summary of the subscription names in use, the subscription types, amount of running instances for each, and the alarm status.

The following are possible CloudWatch alarm states:

- **OK** – The metric or expression is within the defined threshold.
- **ALARM** – The metric or expression is outside of the defined threshold.
- **INSUFFICIENT_DATA** – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.

Topics

- Create a CloudWatch alarm for Linux subscriptions
- Modify a CloudWatch alarm for Linux subscriptions
- Delete a CloudWatch alarm for Linux subscriptions

Create a CloudWatch alarm for Linux subscriptions

You can create alarms for each commercial Linux subscription that you have discovered on your running EC2 instances. If necessary, you can create multiple alarms with different dimensions and conditions for each subscription.

To create a CloudWatch alarm for Linux subscriptions from the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.

2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription to create an alarm for, then choose **Create alarm**.
4. Specify the following for the alarm:
   - **Alarm name** – specify a name which resembles `AWS-LM-LS-AlarmName`.
   - Instance type – choose an instance type that will be using the subscription that was selected.
   - Usage Region – choose the Regions to create the alarms for.
   - Comparison operator – the comparison operator for the alarm threshold.
   - Alarm threshold value – the value for the alarm threshold.
5. Choose **Create** to create the alarm.

Modify a CloudWatch alarm for Linux subscriptions

You can modify existing CloudWatch alarms from the License Manager console to adapt to changing requirements.

To modify a CloudWatch alarm for Linux subscriptions from the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription to modify, then choose **Edit**.
4. Modify the defined values as required.
5. Choose **Edit** to modify the alarm.

Delete a CloudWatch alarm for Linux subscriptions

You can delete existing CloudWatch alarms from the License Manager console to adapt to changing requirements.

To delete a CloudWatch alarm for Linux subscriptions from the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription to modify, then choose **Delete**.

Settings in License Manager

The **Settings** section of the AWS License Manager console displays settings for the current account. You must configure settings to enable associated functionality.

Managed licenses

The following settings are configurable for managed licenses:

- Distribution of managed entitlements and self-managed licenses to your organization
- Cross-account resource discovery
- Amazon SNS notification

For more information, see Managed license settings in License Manager.

Linux subscriptions

The following settings are configurable for Linux subscriptions:

- Discovery and aggregation of Commercial Linux license subscription data
- Red Hat Subscription Manager (RHSM) discovery for Linux subscriptions

For more information, see Linux subscription settings in License Manager.

User-based subscriptions

The following settings are configurable for user-based subscriptions:

- AWS Managed Microsoft AD
- Virtual Private Cloud (VPC)

For more information, see User-based subscription settings in License Manager.

Delegated administration

This tab is displayed if your account has administrative access for your organization. As an administrator, you can register a delegated administrator from the AWS CLI or AWS Management Console. For more information, see Delegated administrator settings in License Manager.

Settings topics

- Edit License Manager settings
- Managed license settings in License Manager
  - Account details
  - Cross-account resource discovery
  - Simple Notification Service (SNS)
- Linux subscription settings in License Manager
  - Linux subscriptions settings
  - Red Hat Subscription Manager discovery
- User-based subscription settings in License Manager
  - AWS Managed Microsoft AD
  - Virtual private cloud
- Delegated administrator settings in License Manager
  - Regions supported for delegated License Manager administrators
  - Register a delegated License Manager administrator
  - Deregister a delegated License Manager administrator

Edit License Manager settings

To edit your License Manager settings, follow these steps:

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Settings**.
3. Choose the tab containing the settings to configure. For example, choose **Managed licenses** to configure **Account details**.
4. After you've configured your settings, choose **Save**, or choose **Cancel** to back out.

Managed license settings in License Manager

The following settings are available for managed licenses.

Account details

You can review your account details to see information such as the account type, whether accounts in AWS Organizations are linked, the account's License Manager S3 bucket ARN, and the AWS Resource Access Manager share ARN. This section also enables you to link your AWS Organizations accounts.

To distribute managed entitlements or self-managed licenses within your organization, choose **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 and member 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 self-managed licenses. For more information, see the AWS Resource Access Manager User Guide.

To disable this option, call the UpdateServiceSettings API.

Cross-account resource discovery

You can turn on cross-account resource discovery in order to manage license usage across all of your accounts in AWS Organizations.

To enable cross-account resource discovery in your organization, choose **Turn on** for cross-account resource discovery. When you turn on the cross-account resource discovery, AWS Organizations will automatically be linked to perform resource discovery across all of your accounts.

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 your accounts in AWS Organizations.

- AWS Glue to provide a fast query experience.

> **Note**
>
> The following AWS Regions don't require Amazon Athena or AWS Glue to query or aggregate inventory data for Systems Manager inventory to discover software usage:
>
> - Asia Pacific (Jakarta)
> - Israel (Tel Aviv)

Simple Notification Service (SNS)

You can configure an Amazon SNS to receive notifications and alerts from License Manager.

To configure an Amazon SNS topic

1. Choose **Edit** next to **Simple Notification Service (SNS)**.
2. Specify an SNS topic ARN in the following format:

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

3. Choose **Save changes**.

Linux subscription settings in License Manager

During the process of discovery, License Manager searches the EC2 instances that are running under your AWS account for Linux subscriptions. It detects if you have more than one Linux subscription defined for any instances, and aggregates the data.

Linux subscriptions settings

You can configure settings for Linux subscriptions to control how License Manager handles discovery and aggregation. Default discovery settings apply across all types of Linux subscriptions.

The following actions are available to configure Linux subscription discovery.

Edit

Change settings for Linux subscription discovery.

Deactivate

Deactivate discovery and aggregation for Linux subscriptions associated with your EC2 instances. If you also have discovery activated for Red Hat Subscription Manager, License Manager first deactivates your RHSM registered provider, then it continues with deactivation for Linux subscription discovery.

> **Note**
>
> Deactivation doesn't affect your access secret for Red Hat Subscription Manager (RHSM). To avoid charges on your AWS bill for an associated secret that you no longer need, see Delete an AWS Secrets Manager secret in the *AWS Secrets Manager User Guide*.

The following settings are displayed in the License Manager console for Linux subscription discovery.

Linux subscription discovery settings

Linux subscription discovery

Indicates whether you've activated Linux subscription discovery for your account.

Source AWS Regions

AWS Regions where you want License Manager to discover subscription data.

AWS Organizations

Optionally aggregate subscription data across your accounts in AWS Organizations.

For more information, see Manage Linux subscriptions in License Manager.

Red Hat Subscription Manager discovery

If you've activated Linux subscription discovery, you can configure access for License Manager to retrieve additional data for RHEL subscriptions that are managed through Red Hat Subscription Manager (RHSM).

The following actions are available to configure your RHSM subscription discovery.

Edit tags

Change the tags that are associated with your access secret.

> **Note**
>
> If you need to make other changes to your RHSM subscription, you must deactivate your current registration first, then set up a new registration.

Deactivate

Deactivate your RHSM registered provider.

> **Note**
>
> Deactivation doesn't affect your access secret for Red Hat Subscription Manager (RHSM). To avoid charges on your AWS bill for an associated secret that you no longer need, see Delete an AWS Secrets Manager secret in the *AWS Secrets Manager User Guide*.

The following settings are displayed in the License Manager console for RHSM discovery.

Red Hat Subscription Manager discovery settings

Discovery status

Indicates whether you've activated discovery for RHSM subscriptions.

Secret name

Links to the RHSM access secret in AWS Secrets Manager that contains your Red Hat offline token. License Manager uses this secret to generate a new temporary access token to request subscription data from Red Hat Subscription Manager (RHSM).

You can make changes to an existing secret through Secrets Manager. To update tags or other metadata for your secret, see Modify an AWS Secrets Manager secret in the *AWS Secrets Manager User Guide*. To update the secret value, see Update the value for an AWS Secrets Manager secret.

Last data synchronized on

The timestamp from the last successful update of subscription data from the registered Red Hat Subscription Manager (RHSM) account.

Tags

You can define key value pairs for tags that License Manager assigns to your RHSM access secret in Secrets Manager. To retrieve and decrypt your RHSM access secret, the License Manager service-linked role policy requires the secret, and any associated AWS KMS key, to have the following tag assigned:

```
"LicenseManagerLinuxSubscriptions": "enabled"
```

The tag is automatically assigned if License Manager created your secret during the registration process. If you create your own secret for the offline token, make sure that you assign that tag to the secret and to the associated KMS key, if it's encrypted. To add the tag, see Modify an AWS Secrets Manager secret in the *AWS Secrets Manager User Guide*.

User-based subscription settings in License Manager

The following settings are available depending on which products you require for user-based subscriptions.

AWS Managed Microsoft AD

License Manager requires AWS Managed Microsoft AD to be configured before you can work with user-based subscriptions. For more information, see Use License Manager user-based subscriptions for supported software products.

Virtual private cloud

License Manager requires your VPC to be configured, in addition to your AWS Managed Microsoft AD, when you use user-based subscriptions with Microsoft Office. For more information, see Use License Manager user-based subscriptions for supported software products.

Delegated administrator settings in License Manager

You can register a delegated administrator to perform administrative tasks for managed licenses and Linux subscriptions in License Manager. To simplify administration, we recommend using the License Manager console to register a single delegated administrator for each feature of License Manager. When you use this approach, you will have a single delegated administrator in your organization for License Manager.

Using the AWS CLI or SDKs, you can register different member accounts in your organization as the delegated administrator for each supported feature of License Manager. This results in different member accounts in your organization being able to perform administrative tasks for managed licenses and Linux subscriptions.

> **Important**
>
> To use the delegated administration features in the License Manager console, you must have the same member account registered as the delegated administrator for each feature of License Manager. If you registered more than one member account as the delegated administrator, you first have to deregister the existing member accounts, and then register the same account for each feature of License Manager.

Before you register a delegated administrator, you must enable trusted access with Organizations. For more information, see Inviting an AWS account to join your organization and Enable trusted access with AWS Organizations.

The following are the features for which you can register a delegated administrator:

Managed licenses

You can perform administrative tasks, such as sharing self-managed licenses with other member accounts, performing cross-account resource discovery, and distributing managed entitlements to other member accounts.

Linux subscriptions

You can perform administrative tasks, such as viewing and managing commercial Linux subscriptions you own and run across AWS Regions and your accounts in AWS Organizations. You can also create and manage Amazon CloudWatch alarms for your Linux subscriptions. The data must first be discovered and aggregated before it is visible in the License Manager console and any alarms can function if they are configured.

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

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

Regions supported for delegated License Manager administrators

The following 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)

Register a delegated License Manager administrator

You can register a delegated administrator using the AWS CLI or AWS Management Console.

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. Choose the **Delegated administration** tab.
5. Choose **Register delegated administrator**.
6. Enter the member account ID to register as the delegated administrator, confirm that you want to grant License Manager the required permissions, and then choose **Register**.
7. A message indicates if the specified account has been successfully registered as the delegated administrator License Manager.

AWS CLI

To register a delegated administrator for managed licenses 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
```

To register a delegated administrator for Linux subscriptions 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-linux-subscriptions.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-linux-subscriptions.amazonaws.com
```

Deregister a delegated License Manager administrator

You can deregister a delegated administrator using the AWS CLI or AWS Management Console.

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. Choose the **Delegated administration** tab.
5. Choose **Remove**.
6. Enter the text **`remove`** to confirm you would like to remove the delegated administrator for License Manager and choose **Remove**.

7. A message indicates if the specified account has been successfully removed the delegated administrator for License Manager.

AWS CLI

To deregister a delegated administrator for managed licenses 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
```

To deregister a delegated administrator for Linux subscriptions 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-linux-subscriptions.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-linux-subscriptions.amazonaws.com
```

You can register a deregistered account again at any time.

Dashboard in License Manager

The **Dashboard** section of the License Manager console provides usage details that you can use to track the license consumption associated with the following:

- Self-managed licenses
- Granted license entitlements
- Subscribed users of user-based subscriptions
- Running instances

The dashboard also displays alerts resulting from license rule violations.

Overview

The overview section provides the following details about your licenses:

Granted licenses

The total amount of granted licenses in this account in this Region.

Self-managed licenses

The total amount of self-managed licenses in this account in this Region.

Seller-issued licenses

The total amount of seller-issued licenses in this account in this Region.

Products

The products section provides the following details for user-based subscriptions.

Product name

The name product of the user-based subscription.

Subscribed users

The amount of subscribed users for the product.

Granted license entitlements

The granted license entitlements section provides the following details.

Product name

The product name of the granted license.

Entitlement

The name of the entitlement.

Usage

The utilization of the entitlement.

Self-managed licenses

The self-managed licenses provides following details.

License name

The name of the self-managed license.

Entitlement

The name of the entitlement.

Usage

The utilization of the entitlement.

Instance usage

The instance usage section provides the following details.

Running instance count

The total amount of running instances in this account in this Region.

Aggregate running instance count

The total amount of running instances aggregated across all of your accounts in AWS Organizations in this Region. This graph is only visible from the management account and delegated administrator account.

Monitoring License Manager

You can monitor the usage of licenses and subscriptions tracked in AWS License Manager using Amazon CloudWatch. CloudWatch collects raw data and processes it into readable, near real-time metrics. You can set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see Monitoring License Manager license usage with Amazon CloudWatch.

You can capture API calls and related events made by or on behalf of your AWS account using AWS CloudTrail. Events are captured as log files and delivered to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see Logging AWS License Manager API calls using AWS CloudTrail.

Contents

- Monitoring License Manager license usage with Amazon CloudWatch
  - Creating alarms to monitor License Manager metrics
- Logging AWS License Manager API calls using AWS CloudTrail
  - License Manager information in CloudTrail
  - Understanding License Manager log file entries

Monitoring License Manager license usage with Amazon CloudWatch

You can monitor metric statistics for License Manager by using Amazon CloudWatch. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can set alarms that watch for certain thresholds and send notifications or take actions when those thresholds are met. For example, you can watch for the percentage of licenses using the `LicenseConfigurationUsagePercentage` metric, and take action before limits are exceeded. For more information, see the Amazon CloudWatch User Guide.

License Manager emits the following metrics hourly in the `AWSLicenseManager/licenseUsage` namespace:

Metric	Description
RunningInstancesCount	The total number of instances running in the current account that are grouped by the subscription name. Units: Count Dimensions: `SubscriptionName` : The name of the subscription.
AggregateRunningInstancesCount	The aggregated total number of instances that are running across all of your accounts in AWS Organizations in the current AWS Region. Units: Count Dimensions: `SubscriptionName` : The name of the subscription.
TotalLicenseConfigurationUsageCount	The total number of a license configuration that could be available. Units: Count Dimensions: • `LicenseConfigurationArn` : The license configuration Amazon Resource Name (ARN). • `LicenseConfigurationType` : The license configuration type.
LicenseConfigurationUsageCount	The total number of used licenses of this configuration. Units: Count Dimensions: • `LicenseConfigurationArn` : The license configuration ARN. • `LicenseConfigurationType` : The license configuration type.
LicenseConfigurationUsagePercentage	The used licenses of this license configuration expressed as a percentage.

Metric	Description
	Units: Percent Dimensions: • `LicenseConfigurationArn` : The license configuration ARN. • `LicenseConfigurationType` : The license configuration type.

Creating alarms to monitor License Manager metrics

You can create a CloudWatch alarm that sends an Amazon Simple Notification Service (Amazon SNS) message when the value of the metric changes and causes the alarm to change state. An alarm watches a metric over a time period you specify, and performs actions based on the value of the metric relative to a given threshold over a number of time periods. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see Using CloudWatch alarms.

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.

Topics

- License Manager information in CloudTrail
- Understanding License Manager log file entries

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 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::123456789012: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":"aws-cli/2.4.6 Python/3.8.8 Linux",
   "requestParameters":{
      "licenseConfigurationArn":"arn:aws:license-manager:us-
east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
   },
   "responseElements":null,
   "requestID":"3366df5f-4166-415f-9437-c38EXAMPLE48",
   "eventID":"6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
   "eventType":"AwsApiCall",
   "recipientAccountId":"012345678901"
}
```

Security in 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 License Manager
- Identity and access management for License Manager
- Using service-linked roles for License Manager
- AWS managed policies for License Manager
- Cryptographic signing of licenses in License Manager
- Compliance validation for License Manager
- Resilience in License Manager
- Infrastructure security in License Manager
- License Manager and interface VPC endpoints with AWS PrivateLink

Data protection in 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. You are also responsible for 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 users with AWS IAM Identity Center or 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 require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- 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 sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 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) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text 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 text 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 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, users don't have permissions for License Manager resources and operations. To allow users to manage License Manager resources, you must create an IAM policy that explicitly grants them 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.

Create users, groups, and roles

You can create users and groups for your AWS account and then assign them the permissions they require. As a best practice, users should acquire the permissions by assuming IAM roles. For more information on how to set up users and groups for your AWS account, see Get started with License Manager.

An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

IAM 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, 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.

Create IAM policies for License Manager

In an IAM policy statement, you can specify any API operation from any service that supports IAM. License Manager, uses the following prefixes with the name of the API operation:

- `license-manager:`
- `license-manager-user-subscriptions:`

- `license-manager-linux-subscriptions:`

For example:

- `license-manager:CreateLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`
- `license-manager-user-subscriptions:ListIdentityProviders`
- `license-manager-linux-subscriptions:ListLinuxSubscriptionInstances`

For more information on the available License Manager APIs, see the following API references:

- AWS License Manager API Reference
- AWS License Manager User Subscriptions API Reference
- AWS License Manager Linux Subscriptions API Reference

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:*"
```

Example policy for an ISV using License Manager

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

JSON

```
{
    "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": "*"
        }
    ]
}
```

Grant permissions to users, groups, and roles

Once you have created the IAM policies you require, you must grant these permissions to your users, groups, and roles.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.
- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Using service-linked roles for 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 – Management account role
- License Manager – Member account role
- License Manager – User-based subscription role
- License Manager – Linux subscriptions role

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.

To review permissions for the **AWSLicenseManagerServiceRolePolicy**, see AWS managed policy: AWSLicenseManagerServiceRolePolicy. To learn more about configuring permissions for a service-linked role, 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 the 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 doesn't 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 self-managed licenses from associated instances and AMIs, and then deleting the self-managed licenses.

> **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 **Self-managed licenses**.
3. Choose a self-managed license for which you are the owner and disassociate all entries within the **Associated AMIs** and **Resources** tabs. Repeat this process for each license configuration.
4. While still on the self-managed license's page, choose **Actions**, then choose **Delete**.
5. Repeat the previous steps until all self-managed licenses 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 AWSServiceRoleForAWSLicenseManagerMasterAccountRole and AWSLicenseManagerMemberAccountRole, 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.

To review permissions for the **AWSLicenseManagerMasterAccountRolePolicy**, see AWS managed policy: AWSLicenseManagerMasterAccountRolePolicy. To learn more about configuring permissions for a service-linked role, 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 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 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.

To review permissions for the **AWSLicenseManagerMemberAccountRolePolicy**, see AWS managed policy: AWSLicenseManagerMemberAccountRolePolicy. To learn more about configuring permissions for a service-linked role, 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 the AWS 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 the service-linked role

1. Log in to 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**, and then choose **Edit**.
4. Choose **Link AWS Organizations accounts**.
5. Choose **Apply**. This creates the roles AWSServiceRoleForAWSLicenseManagerRole and AWSServiceRoleForAWSLicenseManagerMemberAccountRole 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*.

License Manager – User-based subscription role

License Manager requires a service-linked role for managing AWS resources that will provide user-based subscriptions.

Permissions for the user-based subscription role

The service-linked role named `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` allows License Manager to utilize AWS Systems Manager and manage Amazon EC2 resources providing user-based subscriptions, as well as describe AWS Directory Service resources.

To review permissions for the **AWSLicenseManagerUserSubscriptionsServiceRolePolicy**, see AWS managed policy: AWSLicenseManagerUserSubscriptionsServiceRolePolicy. To learn more about configuring permissions for a service-linked role, 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 as you will be prompted on the License Manager console **User-based subscriptions** pages to create the role.

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*.

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

To create the service-linked role

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **User Association** or **Products**.
3. Agree to the terms for License Manager to create the user-based subscription role.
4. Choose **Create**. This creates the role.

You can also use the IAM console to create a service-linked role with the `License Manager - User-based subscriptions` use case. Alternatively, in the AWS CLI or AWS API, create a service-linked role with the `license-manager-user-subscriptions.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 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` 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 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

License Manager – Linux subscriptions role

License Manager requires a service-linked role to manage AWS resources that provide Linux subscriptions.

Permissions for the Linux subscriptions role

The service-linked role named `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` allows License Manager to perform the following actions for Linux subscriptions.

- Discover Amazon Elastic Compute Cloud and AWS Organizations resources.
- Retrieve secrets tagged with `"LicenseManagerLinuxSubscriptions": "enabled"` from AWS Secrets Manager for access to third-party Linux subscription providers to get subscription information.
- Use KMS keys tagged with `"LicenseManagerLinuxSubscriptions": "enabled"` to decrypt secrets.

To review permissions for the **AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy**, see AWS managed policy: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy. To learn more about configuring permissions for a service-linked role, 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 as you will be prompted on the License Manager console **Linux subscriptions** pages to create the role.

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*.

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

To create the service-linked role

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the left navigation pane, choose **Subscriptions** or **Instances**.
3. Agree to the terms for License Manager to create the Linux subscriptions role.
4. Choose **Create**. This creates the role.

You can also use the IAM console to create a service-linked role with the `License Manager - Linux subscriptions` use case. Alternatively, in the AWS CLI or AWS API, create a service-linked role with the `license-manager-linux-subscriptions.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 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 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 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

AWS managed policies for 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 about the service-linked role, see Permissions for the core 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/AWSServiceRoleForMarketplaceLicenseManagement`
`iam:CreateServiceLinkedRole`	`arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole`

Action	Resource ARN
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	*

Action	Resource ARN
`license-manager:GetLicense*`	*
`license-manager:UpdateLicenseSpecificationsForResource`	*
`license-manager:List*`	*

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

AWS managed policy: AWSLicenseManagerMasterAccountRolePolicy

This policy is attached to the service-linked role named `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` to allow License Manager to call API actions that perform license management for a central management account on your behalf. For more information about the service-linked role, see License Manager – Management account 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-*`

Action	Resource ARN
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-*
s3:DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	See footnote [1]

Action	Resource ARN
glue:UpdateTable	See footnote [1]
glue:DeleteTable	See footnote [1]
glue:UpdateJob	See footnote [1]
glue:UpdateCrawler	See footnote [1]
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	*

Action	Resource ARN
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DeleteStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

[1] The following are the resources defined 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

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

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 License Manager – Member account role.

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

Action	Resource ARN
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:GetLicenseConfiguration	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:CreateResourceDataSync	*
ssm:DeleteResourceDataSync	*

Action	Resource ARN
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

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

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 Seller issued license usage in License Manager.

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

AWS managed policy: AWSLicenseManagerUserSubscriptionsServiceRolePolicy

This policy is attached to the service-linked role named AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService policy to allow License Manager to call API actions to manage user-based subscription resources. For more information, see License Manager – User-based subscription role.

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

Action	Resource ARN
ds:DescribeDirectories	*
ds:GetAuthorizedApplicationDetails	*

Action	Resource ARN
ec2:CreateTags	arn:aws:ec2:*:*:instance/* [1]
ec2:DescribeInstances	*
ec2:DescribeNetworkInterfaces	*
ec2:DescribeSecurityGroupRules	*
ec2:DescribeSubnets	*
ec2:DescribeVpcPeeringConnections	*
ec2:TerminateInstances	arn:aws:ec2:*:*:instance/* [1]
route53:GetHostedZone	*
route53:ListResourceRecordSets	*
secretsmanager:GetSecretValue	arn:aws:secretsmanager:*:*:secret:license-manager-user-*
ssm:DescribeInstanceInformation	*
ssm:GetCommandInvocation	*
ssm:GetInventory	*
ssm:ListCommandInvocations	*
ssm:SendCommand	arn:aws:ssm:*::document/AWS-RunPowerShellScript [2] arn:aws:ec2:*:*:instance/* [2]

[1] License Manager can only create tags on and terminate instances which have the product codes bz0vcy31ooqlzk5tsash4r1ik, 77yzkpa7kvee1y1tt7wnsdwoc, or d44g89hc0gp9jdzm99rznthpw.

[2] License Manager can only execute an SSM Run Command with the `AWS-RunPowerShellScript` document on instances with the tag name of `AWSLicenseManager` and a value of `UserSubscriptions`.

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

AWS managed policy: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

This policy is attached to the service-linked role named `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` policy to allow License Manager to call API actions to manage Linux subscriptions resources. For more information, see License Manager – Linux subscriptions role.

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

Action	Conditions	Resource
`ec2:DescribeInstances`	N/A	*
`ec2:DescribeRegions`	N/A	*
`organizations:DescribeOrganization`	N/A	*
`organizations:ListAccounts`	N/A	*
`organizations:DescribeAccount`	N/A	*
`organizations:ListChildren`	N/A	*
`organizations:ListParents`	N/A	*

Action	Conditions	Resource
`organizations:ListAccountsForParent`	N/A	*
`organizations:ListRoots`	N/A	*
`organizations:ListAWSServiceAccessForOrganization`	N/A	*
`organizations:ListDelegatedAdministrators`	N/A	*
secretsmanager:GetSecretValue	StringEquals: *"aws:ResourceTag/LicenseManagerLinuxSubscriptions": "enabled"* *"aws:ResourceAccount": "${aws:PrincipalAccount}"*	`arn:aws:secretsmanager:*:*:secret:*`
kms:Decrypt	StringEquals: *"aws:ResourceTag/LicenseManagerLinuxSubscriptions": "enabled",* *"aws:ResourceAccount": "${aws:PrincipalAccount}"* StringLike: *"kms:ViaService": ["secretsmanager.*.amazonaws.com"]*	`arn:aws:kms:*:*:key/*`

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

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.

Change	Description	Date
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – Update to an existing policy	License Manager added the following permissions to manage licensing and Active Directory data: get route information from Route 53, get networking information and security group rules from Amazon EC2, and get secrets from Secrets Manager.	November 7, 2024
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – Update to an existing policy	License Manager added permissions to store and retrieve secrets from AWS Secrets Manager, and to use AWS KMS keys to decrypt access token secrets for Bring Your Own License (BYOL) subscriptions.	May 22, 2024
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – New policy	License Manager added a permission to create the service-linked role named `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` . This role provides License Manager permission to list AWS Organizations and Amazon EC2 resources.	December 21, 2022

Change	Description	Date
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – Update to an existing policy	License Manager added the `ec2:DescribeVpcPeeringConnections` permission.	November 28, 2022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – New policy	License Manager added a permission to create the service-linked role named `AWSLicenseManagerUserSubscriptionsServiceRolePolicy` . This role provides License Manager permission to list AWS Directory Service resources , utilize Systems Manager features, and manage Amazon EC2 resources created for user-based subscriptions.	July 18, 2022
AWSLicenseManagerMasterAccountRolePolicy – Update to an existing policy	License Manager added the `resource-groups:PutGroupPolicy` permission for resource groups managed by AWS Resource Access Manager.	June 27, 2022

Change	Description	Date
AWSLicenseManagerMasterAccountRolePolicy – Update to an existing policy	License Manager changed the AWS managed policy `AWSLicenseManagerMasterAccountRolePolicy` condition key for AWS Resource Access Manager from using `ram:ResourceTag` to `aws:ResourceTag` .	November 16, 2021
AWSLicenseManagerConsumptionPolicy – New policy	License Manager added a new policy that grants permissions to consume licenses.	August 11, 2021
AWSLicenseManagerServiceRolePolicy – 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 – 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 – 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 in License Manager

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 AWS KMS key 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::123456789012:license:l-6585590917ad46858328ff02dEXAMPLE",
   "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
   "nodeId":"100.20.15.10",
   "checkoutMetadata":{
      "Mac":"ABCDEFGHI"
   }
}
```

Compliance validation for License Manager

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. 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 Compliance & Governance – These solution implementation guides discuss architectural considerations and provide steps for deploying security and compliance features.
- HIPAA Eligible Services Reference – Lists HIPAA eligible services. Not all AWS services are HIPAA eligible.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Customer Compliance Guides – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).
- 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. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- Amazon GuardDuty – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.

- 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 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 License Manager

As a managed service, AWS License Manager is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access License Manager through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by 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.

License Manager and interface VPC endpoints with 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 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 the section called "Settings".

Cross-account discovery error

While setting up cross-account discovery, you may encounter the following error message on the **Inventory search** 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.

Management account cannot disassociate resources from a self-managed license

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 self-managed license, 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 self-managed licenses once every few hours. If an AMI associated with a self-managed license 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 self-managed license 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 self-managed license 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.

User subscription product configuration failing

Your product configuration may be failing due to issues with outbound network access. To address this, ensure that the default security group permits outbound traffic to the IPv4 addresses of each domain controller's network interface as well as SSM.

- Verify that default security group settings facilitate outbound traffic to the IPv4 addresses of domain controller network interfaces.
  - License Manager creates two network interfaces which use the default security group of the VPC where your AWS Managed Microsoft AD is provisioned. These interfaces are used for required service functionality with your directory. Ensure that your default security group allows outbound traffic to each domain controller's network interface IPv4 address, or the security group used by the domain controllers. For more information, see Prerequisites to create user-based subscriptions and What gets created in the AWS Directory Service Administration Guide.
- Configure outbound internet access from instances providing user-based subscriptions or VPC endpoints.
  - Outbound internet access from the instances providing user-based subscriptions, or VPC endpoints, must be configured for your instances to communicate with SSM. For more information, see Setting up Systems Manager for EC2 instances in the AWS Systems Manager User Guide.

Once the provisioning process is complete, you can associate a different security group to the interfaces created by License Manager. The security group you select must also allow the required traffic to each domain controller's network interface IPv4 address or security group. For more information, see Work with security groups in the Amazon Virtual Private Cloud User Guide.

User subscription instances failing to launch

Your instance launches can be failing due to multiple reasons. Here are some of the common issues for which an instance launch may fail:

- Ensure your instance is discoverable by SSM, see the section called “Troubleshoot instance connectivity”.
- Ensure your instance is able to join your domain, see the section called “Troubleshoot failures to join the domain”.
- Ensure that the Route53 outbound resolver endpoint rule is set. For more information, see the blog post Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolvers.
- If launching instances from custom AMIs created on top of User subscription AMIs, please make sure to perform Sysprep and ensure unique computer names when creating and launching instances from custom AMIs.

Seamless domain join for EC2 instances with user subscription products doesn't work

License Manager needs to perform domain join on these instances using SSM to allow authorized access to only users subscribed to the product. As a result, the seamless domain join feature is deactivated.

Unable to delete active directory

License Manager is registered as an authorized application with Directory Service during configuration, thereby safeguarding active directories from deletion once configured. As part of the standard procedure, customers need to first remove all instances, instance associations, and user subscriptions. Following this, they can proceed with removing the active directory from the License Manager and subsequently delete the directory itself.

VPC endpoint was created in my account

License Manager creates VPC endpoints required for your resources to connect to activation servers and remain in compliance when you configure your VPC.

Remove all VPC endpoint resources created by License Manager

In order to delete the VPC endpoint resources, you must perform the following actions:

- Disassociate all users from their user-based subscriptions. For more information, see the section called “Disassociate users from an instance”.
- Remove any directory that is configured from the License Manager settings. For more information, see the section called “Deregister Active Directory”.
- Terminate all instances providing user-based subscription products. For more information, see the section called “Launch an instance from a license included AMI”.

Unable to delete AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service Linked Role (SLR)

License Manager requires the "AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService" service-linked role for managing AWS resources that will provide user-based subscriptions. 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.

For more information, see the section called “User-based subscription prerequisites” and License Manager – User-based subscription role and Service-linked roles.

Subscription is not present error for RDS SAL product

Your account must have a subscription to Windows Server Remote Desktop Services Subscriber Access License (RDS SAL). All users associated with instances providing user-based subscription products must have a single active subscription to this license in addition to any other products

they would like to use. Your user will be subscribed to RDS SAL on their behalf when they subscribe to a user-based subscription product.

But if this has been unsubscribed or removed due to other compliance reasons, you might have to resubscribe. If you are already subscribed, you can try unsubscribing and resubscribing, which will not affect your License Manager user subscriptions.

Troubleshooting trusts

Based on our experience working with many customers, the vast majority of trust configuration issues are either DNS resolution or networking connectivity errors. These are some troubleshooting steps to help you resolve common issues:

- Check whether you allowed outbound networking traffic on the AWS Managed Microsoft AD.
- If the DNS server or the network for your on-premises domain uses a public (non-RFC 1918) IP address space, follow these steps:
  - In the AWS Directory Service console, go to the IP routing section for your directory, choose **Actions**, and then choose **Add route**.
  - Enter the IP address block of your DNS server or on-premises network using CIDR format, for example 203.0.113.0/24.
  - This step isn't necessary if both your DNS server and your on-premises network are using RFC 1918 private IP address spaces.
- After you verify the security group and check whether any applicable routes are required, launch a Windows Server instance and join it to the AWS Managed Microsoft AD directory. Once the instance is launched:
  - Run this PowerShell command to test DNS connectivity:

```
Resolve-DnsName -Name 'example.local' -DnsOnly
```

You should also look through the message explanations in the Trust creation status reasons guide in the AWS Directory Service documentation.

Billing issues for user subscriptions

AWS will bill you through a monthly subscription, based on the number of users associated with the license included Microsoft Office or Visual Studio instances. These per-user charges are billed

per calendar month, and the billing starts from the time you subscribe to the product. If you remove access to a user during the existing month, you will be billed for the user for the remainder of the month. You will stop incurring charges for the user the following month.

Furthermore:

- Billing is based on a per-user basis within User subscriptions. Only users who are subscribed to the product will incur charges, not all users in the active directory.
- Billing operates on a monthly cycle, starting from the first day of each calendar month. Charges are levied for the entire month, regardless of the specific date of subscription activation.
- You need an RDS SAL for each user who needs to access your Office/VS instances.
- To stop incurring charges for user-based subscriptions, you must disassociate the user from all instances they are associated with. Deleting a user from Active Directory does not disassociate the user from instances. For more information, see the section called “Disassociate users from an instance”.
- A user is only counted once. You get charged per user for Microsoft Office and Visual Studio, irrespective of the number of EC2 instances the user connects to. Users are charged for their subscription once, regardless of their usage of multiple instances.

User subscription products show Marketplace subscription status of Inactive

After you configure your directory with the required products, you would need to subscribe to the required products. Products with a Marketplace Subscription Status of Inactive require you to subscribe before you can associate users to an instance and utilize them.

Change a username on Managed Active Directory

Changing a username has no effect on their ability to RDP into associated instances. The associated users should be able to use their updated login details to RDP into user subscription instances.

Dissociate users from a terminated instance

Whenever a user subscriptions instance is terminated, all the users that are associated to the instance are disassociated. You do not have to manually disassociate the user.

> **Note**
>
> Users are not dissociated if the instance is stopped.

User limits per instance

There is a limit of 25 instances per user. In case you need adjustment, please reach out to AWS Support. Users are charged for their subscription once, regardless of their usage of multiple instances.

Installing additional software on user subscription instances

You can install additional software on your instances that aren't available as user-based subscriptions. Additional software installations aren't tracked by License Manager. These installations must be performed using the Admin account which is created by default in your AWS Managed Microsoft AD directory. For more information, see Admin account in the AWS Directory Service Administration Guide.

To install additional software with the Admin account, you must:

- Subscribe the Admin account to the product provided by the instance.
- Associate the Admin account to the instance.
- Connect to the instance using the Admin account to perform the installation.

For more information, see the section called “Get started”.

Japanese Language Packs on user subscription instances

Japanese language pack installation is supported with User subscription instances.

Local Administrator user on user subscription instances

We only allow users under the users managed active directory domain to be associated with user subscription instances to prevent unauthorized access to these Microsoft products. When you create local users with administrator privileges on instances that provide user-based subscriptions, the instance's health status changes to unhealthy.

Unhealthy instances

Instances providing user-based subscriptions must remain in a healthy status to be in compliance. Instances that are marked as unhealthy no longer meet the required prerequisites. License Manager attempts to return the instance to a healthy status, but instances that are not able to return to a healthy status are terminated.

Number of users that can RDP to a user subscriptions instance

Instances that provide user-based subscriptions support up to two active user sessions at a time as stated in Use License Manager user-based subscriptions for supported software products. By default, Windows allows up to 2 Remote Desktop connections including an Admin connection at any given time, in all editions of Windows server. For using more than 2 concurrent users, customers need to setup an RDS Licensing server.

Supported Windows operating systems

For information about supported Windows operating system platforms, see the section called "Supported software subscriptions".

Supported versions of Office and Visual Studio

For information about supported software for user-based subscriptions, see the section called "Supported software".

Using user subscription with older Windows Server versions

When you launch an instance from an AMI that supports Office LTSC Professional Plus or Microsoft Visual Studio, the launch defaults to the latest Windows OS platform version of the AMI (for example Windows Server 2022). To launch with an earlier OS platform version, follow these steps:

1. Open the AWS Marketplace console at https://console.aws.amazon.com/marketplace.
2. Choose **Manage subscriptions** from the navigation pane.
3. To streamline subscription results, you can search for all or part of the subscription name. For example, Office LTSC Professional Plus 2021 or Visual Studio Enterprise.

4. Select **Launch new instance** from the subscription panel. This opens a launch configuration page.
5. To launch an instance from an AMI that's based on an earlier version of the Windows OS platform, select the full AWS Marketplace website link, located under the Software version. This takes you to a configuration page where you can select from a list of versions.
6. The list shows the latest AMI versions for the supported Windows OS platforms. Select the Windows OS version that you want to launch from.

Using License Manager user subscriptions across accounts or regions

These scenarios are not supported:

- Using License Manager user subscriptions across accounts
- Using License Manager user subscriptions across regions
- Using License Manager user subscriptions with shared Active Directory

CAL token handling during migration to RDS SAL

If you use your own Microsoft RDS license servers, any Client Access License (CAL) tokens already issued remain valid until they expire. During this period users with valid CAL tokens are not automatically subscribed to the RDS SAL product. New user sessions are not automatically subscribed to RDS SAL even though License Manager is configured. License Manager does not override existing CAL tokens issued by your own license servers. The service-managed license server begins issuing tokens and handling new requests only after the existing CAL tokens expire. Once the currently issued CAL tokens reach their expiration date, new token requests are handled by the service-managed license server, and users are auto-subscribed to the RDS SAL product as needed.

Users in my self-managed AD with User subscription products

To associate users in your self-managed directory, you must establish a two-way forest trust between your self-managed directory and your AWS Managed Microsoft AD directory. For more information, see Tutorial: Create a trust relationship between your AWS Managed Microsoft AD and your self-managed Active Directory domain in the AWS Directory Service Administration Guide.

Tips for contacting AWS Support

- When contacting AWS support, please create an instance with the same settings as a terminated instance and enable instance termination protection for a quick response.
- For any RDP related issues we would require RDP related logs to help debug these issues. Please utilize the 'AWSSupport-RunEC2RescueForWindowsTool' for environments with internet access. For more information, see EC2Rescue for Windows Server.
- By using an Office instance as a working instance and mounting a volume restored from a snapshot of the original instance's volume, it is possible to collect data even in an environment without internet access.
- Troubleshooting Instance Launches from Backup AMIs: If you launch an instance from a backup AMI, you must terminate the original instance.

Document history for License Manager

The following table describes the releases of AWS License Manager.

Change	Description	Date
Added support for Microsoft Remote Desktop Services Subscriber Access Licenses (RDS SAL) user-based subscriptions	License Manager added support for management and configuration of RDS SAL user-based subscriptions, including the ability to configure more than two remote desktop connections at a time.	November 14, 2024
Updated user-based subscriptions SLR managed policy to get route and networking information	License Manager added the following permissions to manage licensing and Active Directory data: get route information from Route 53, get networking information and security group rules from Amazon EC2, and get secrets from Secrets Manager. For more information, AWS managed policy: AWSLicenseManagerUserSubscriptionsServiceRolePolicy.	November 7, 2024
Retrieve BYOL subscription information from Red Hat Subscription Manager (RHSM)	License Manager added support to retrieve subscription information from RHSM for BYOL licenses on Red Hat Enterprise Linux instances. This includes updates to the AWSLicenseManagerL	July 10, 2024

Change	Description	Date
	inuxSubscriptionsServiceRolePolicy.	
Added support for Amazon RDS for Db2 vCPU-based BYOL licenses	License Manager added support for Amazon RDS for Db2 vCPU-based BYOL licenses.	March 20, 2024
Added Windows Server 2019 support for Microsoft Office user-based subscriptions	AWS added support for Windows Server 2019 in the Amazon Machine Images (AMIs) with Amazon-provided licenses for Microsoft Office LTSC Professional Plus 2021 on Amazon EC2.	December 4, 2023
Self-managed (on-premises) domain users can utilize user-based subscriptions	License Manager added support for users in self-managed active directory domain to utilize user-based subscriptions when a trust with your AWS Managed Microsoft AD directory has been created.	September 6, 2023
License type conversions for Ubuntu LTS subscriptions	License Manager added support for Ubuntu LTS instances to use license type conversion to add a Ubuntu Pro subscription.	April 20, 2023
Replace active grants	License Manager added functionality to optionally replace active grants for a granted license during grant activation.	March 31, 2023

Change	Description	Date
Delegated administration for Linux subscriptions	License Manager added support for delegated administrators for Linux subscriptions.	March 3, 2023
Linux subscriptions	License Manager added tracking for commercial Linux subscriptions.	December 21, 2022
Amazon CloudWatch metrics	License Manager now emits CloudWatch metrics for license configuration usage and subscriptions.	December 21, 2022
Microsoft Office for user-based subscriptions	License Manager added Microsoft Office as supported software for user-based subscriptions.	November 28, 2022
Distribute entitlements to organizational units	Distribute entitlements to specific a specific OU in your organization.	November 17, 2022
Organization wide view (console)	Manage granted licenses across your accounts in AWS Organizations using the License Manager console.	November 11, 2022
User-based subscriptions	Utilize supported user-based subscription products on Amazon EC2.	August 2, 2022
Record and submit license usage data (console)	Record and submit license usage data using the License Manager console.	March 28, 2022

Change	Description	Date
License type conversion (console)	Change your license type between AWS provided licensing and Bring Your Own License model (BYOL) using the License Manager console without redeploying your existing workloads.	November 9, 2021
License type conversion (CLI)	Change your license type between AWS provided licensing and Bring Your Own License model (BYOL) using the AWS CLI without redeploying your existing wor kloads.	September 22, 2021
Sharing entitlements	Share managed license entitlements with your entire organization with one request.	July 16, 2021
Usage reports	Track the history of your license type configurations with License Manager usage reports. Usage reports were formerly called report generators and license reports.	May 18, 2021
Automated discovery exclusion rules	Exclude instances from License Manager automated discovery based on AWS account IDs and tags.	March 5, 2021

Change	Description	Date
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 self-managed licenses 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
Host resource groups	Configure a host resource group to enable License Manager to manage your Dedicated Hosts.	December 1, 2019

Change	Description	Date
Automated software discovery	Configure License Manager to search for newly installed operating systems or applications and attach the corresponding self-managed licenses 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