How to use Managed entitlements for AWS Marketplace

Contents

What is Managed entitlements for AWS Marketplace?

Managed entitlements for AWS Marketplace help buyers automatically create licenses corresponding to product subscriptions across its catalog of more than 8,000 offerings. This gives buyers account-level visibility to their licenses procured in AWS Marketplace and gives buyers the ability to manage and distribute access rights (or entitlements) to those licenses.

Managed entitlements is available for all AWS Marketplace customers with new or existing subscriptions to:

- Amazon Machine Images

- Containers
- Machine Learning Algorithms and Models
- Data Exchange
- *SaaS (Partially supported: licenses are created, but cannot be distributed)*

How does this benefit the customer?

Governance: Managed entitlements for AWS Marketplace helps customers centralized license governance and management to a single account in their AWS Organization.
Scale: Customers can use APIs to automate entitlement distribution across multiple accounts. This automation mitigates the manual subscription step that each end user account would have needed to take in order to get access to the software.
Integration/Interoperability with other AWS tools: Customers can use managed entitlements APIs alongside AWS Service Catalog and AWS Control Tower. They can fully automate account creation, entitlement distribution, and software provisioning.

Where can I manage my AWS MP license entitlements?
You can manage your AWS MP license entitlements in the Granted Licenses section of the AWS License Manager console or via APIs.

Terminology
License: A license is a representation of the customer's subscription and entitlement to a MP product. AWS Marketplace will automatically create a license on behalf of the customer when the customer subscribes to a AMI, Containers, Machine learning, or Data Exchange product.
Entitlement: An entitlement represents the 'right to use' a product. For AWS Marketplace products, this is evaluated at the AWS Account level. The account that subscribes to a MP product will automatically be entitled to that product and can use it immediately. This same account can then choose to grant (share access) entitlement to other accounts in their AWS Organization.
Grant: This is an action invoked on a licenses to share access to other accounts and grant other accounts the ability to use the license. AWS MP customer subscribers can choose to grant license entitlements to other members of their AWS Organization.

Granted License: Granted licenses are shown in the AWS License Manager console. For MP subscribed products these licenses can take one of two forms.

- Subscribed license - A granted license that results directly from a MP product subscription. This license can be subsequently granted to other accounts in the AWS Organization.
- Entitled license - A granted license that results from a 'Create grant' action that an administrator takes to enable an end user to receive access to a MP product.

License Home Region: All license resources are created and managed with us-east-1 (N. Virginia) as their home region. This means that updates and edits to a license must be done in N. Virginia. This does not impact where instances/resources can be launched or deployed.

User Definitions and Management
Grantor or Administrator: This is the user who creates the agreement via subscription to the MP product. This user receives a license from that subscription and can subsequently grant entitlements to that license to other members of their AWS Organization.

- Customers using All Feature Orgs - We highly recommend that you subscribe to MP licenses through your management account. Doing so will allow you to take advantage of additional governance

mechanisms including being able to 'Auto-accept' granted entitlements in linked accounts and being able to distribute to your AWS Organization ID.

Grantee or End User: These are accounts who receive the entitlements granted from the Grantor/Administrator. Once granted, licenses can be accepted and activated by end users without them having to explicitly subscribe through MP again.

Pre-requisite Permissions and explanations

Customers who want to use the managed entitlements feature will need a combination of permissions including enabling service trusted access and service linked roles:

- **Trusted Access:** Only available for AWS Organizations with 'all-features' enabled. AWS services for which you enable trusted access can access your organization information and perform actions in multiple AWS accounts within your organization. Specific to managed entitlements, this gives AWS LM and MP the ability to keep track of AWS Organizations activity on your behalf (e.g. knowing when accounts leave your organization, validating granted licenses to accounts within an organization)

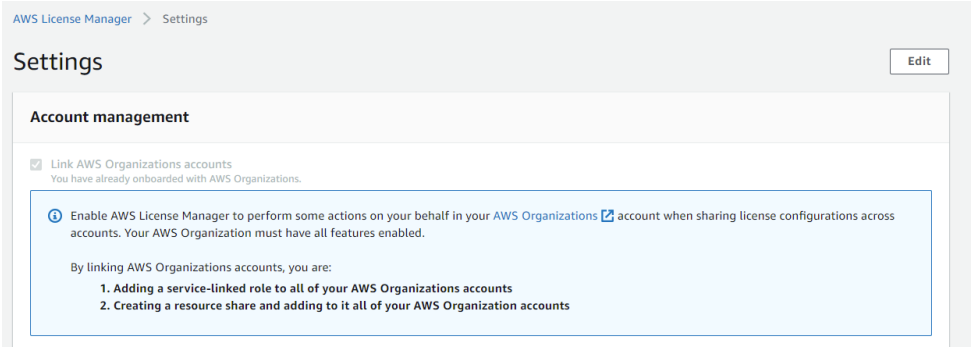
- **Service-Linked Roles**: A service-linked role is a unique type of IAM role that is linked directly to an AWS service. Service-linked roles are predefined by the service and include all the permissions that the service requires to call other AWS services on a customer's behalf. For managed entitlements, this permission is required so that AWS MP can successfully orchestrate license workflows and distributions across multiple AWS services, on the customer's behalf. Similarly, this permission is required for AWS LM to auto-accept grants between management and member accounts in a 'all features' enabled organization.

Pre-requisite Permissions

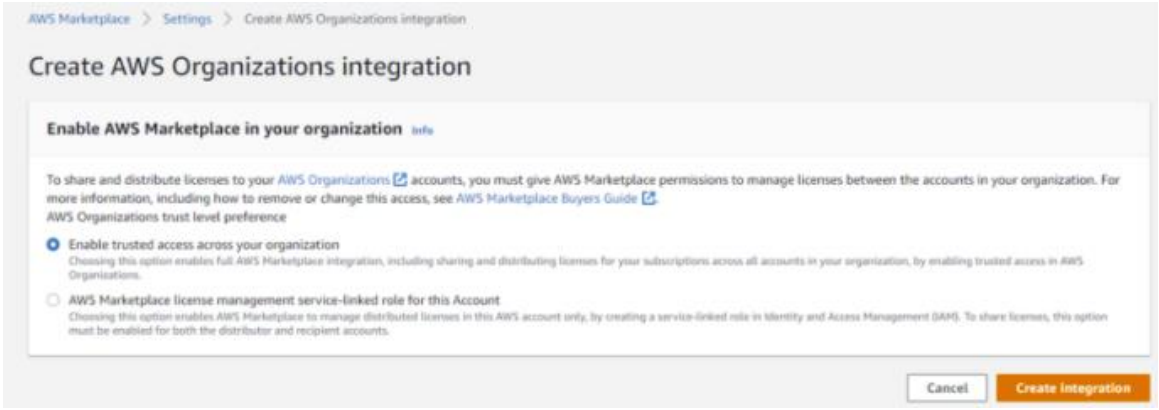
Customers who want to use managed entitlements for AWS Marketplace will first need to set up the following permissions:

AWS Console specific instructions

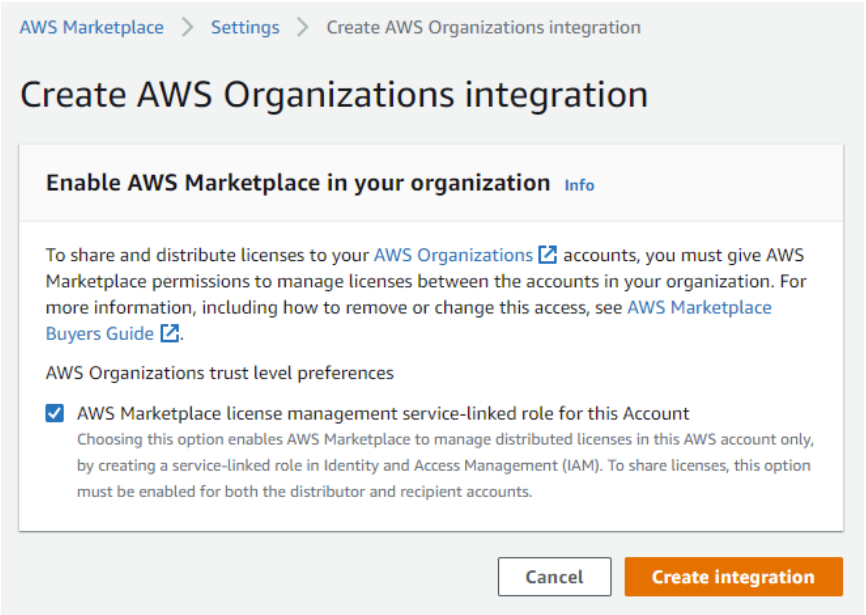
- In an AWS Organization with 'all features' enabled, you will need to create Service Linked Roles (SLR) for AWS License Manager and AWS Marketplace
    - AWS License Manager Console
        - SLR for License Manager will show up as a pop up modal the very first time you enter the LM console. You will not be able to use the AWS License Manager service without first enabling the AWS License Manager SLR.
        - Cross-account SLR for License Manager can be found in the settings page. Using the us-east-1 (N. Virginia) AWS region, select the 'Link AWS Organization accounts' to take advantage of the grant auto-accept feature.
            - This gesture via console also creates a trusted access relationship between AWS Organizations and AWS License Manager



    - AWS Marketplace Console

        - SLR for Marketplace will be available to configure in the Settings page of AWS Marketplace. Select 'Enable trusted access across your organization'
            - This gesture via console also creates a trusted access relationship between AWS Organizations and AWS Marketplace - License Management
        - 

            - Note: As a management account in an all features enabled organization, you can select the 'enable trusted access across your organization' option. This ensures that SLRs will be created for your organization's linked accounts as well. Selecting just the SLR for the individual account will mean that you will need to similarly enable SLR on each linked account you wish to distribute licenses.
- In a consolidated billing organization (if all-features are not enabled), you will need to create Service Linked Roles (SLR) for AWS License Manager and AWS Marketplace
    - AWS License Manager Console
        - SLR for License Manager will show up as a pop up modal the very first time you enter the LM console. You will not be able to use the AWS License Manager service without first enabling the AWS License Manager SLR.
    - AWS Marketplace Console
        - You will need to enable the service linked role for AWS Marketplace - License Management across every account that you plan to grant or receive licenses through managed entitlements.



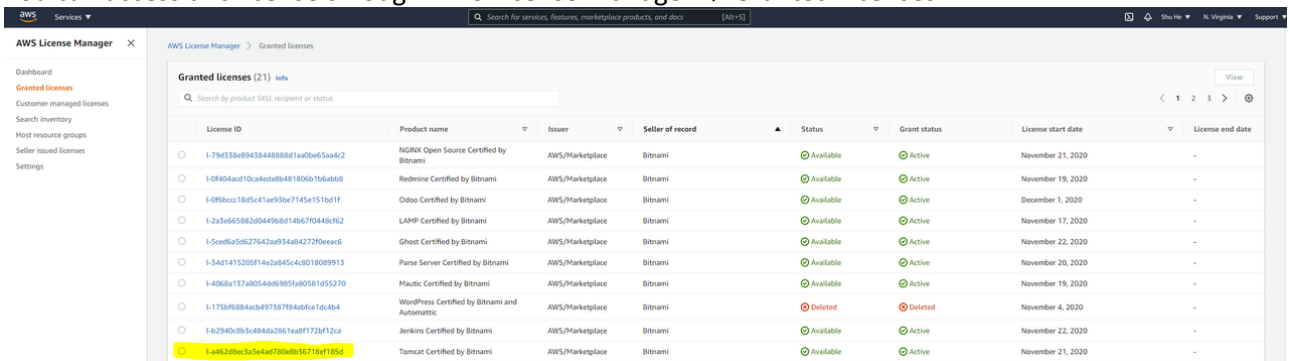
API Specific instructions:

- In an AWS Organization with 'all features' enabled, you will need to use your management account to enable trusted access for your organization.
    - API: EnableAWSServiceAccess
        - AWS Marketplace - License Management
        - AWS License Manager
    - Then create SLRs for AWS Marketplace and AWS License Manager
        - API: CreateServiceLinkedRole
        - AWS License Manager
            - AWSServiceRoleForAWSLicenseManagerRole (needed in all accounts)
            - AWSServiceRoleForAWSLicenseManagerMasterAccountRole (needed only in management account)
            - AWSLicenseManagerMemberAccountRolePolicy (needed in all accounts)
        - AWS Marketplace
            - AWSServiceRoleForMarketplaceLicenseManagement
- In a consolidated billing organization, you will need to create Service Linked Roles (SLR) for AWS License Manager and AWS Marketplace across all accounts where you want to manage entitlements.
    - API: CreateServiceLinkedRole
    - AWS License Manager
        - AWSServiceRoleForAWSLicenseManagerRole
    - AWS Marketplace
        - AWSServiceRoleForMarketplaceLicenseManagement

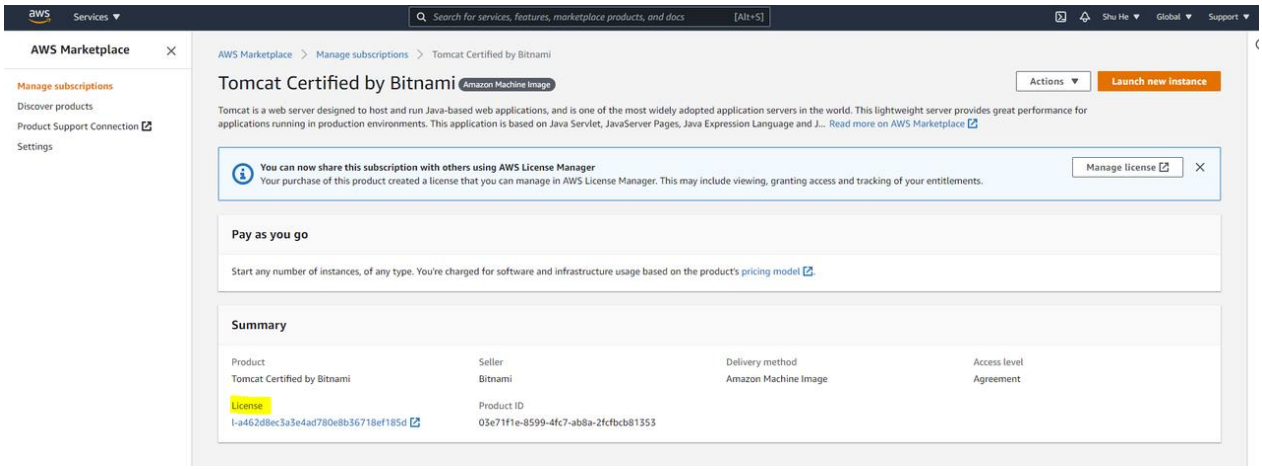
Actions that a managed entitlements Grantor or license Administrator can perform
As a grantor or administrator you can share your MP AMI, Containers, Machine learning, or Data Exchange product to end user AWS Accounts or your AWS Organization ID (available for all-features enabled orgs only)

Specifying an AWS Account
Creating Grants to an AWS Account:
Step 1: Select the product license that you wish to grant

- As a Grantor or Administrator, once you've subscribed to a MP product, a license will automatically be created and granted to you.
- You can access this license through AWS License Manager → Granted Licenses

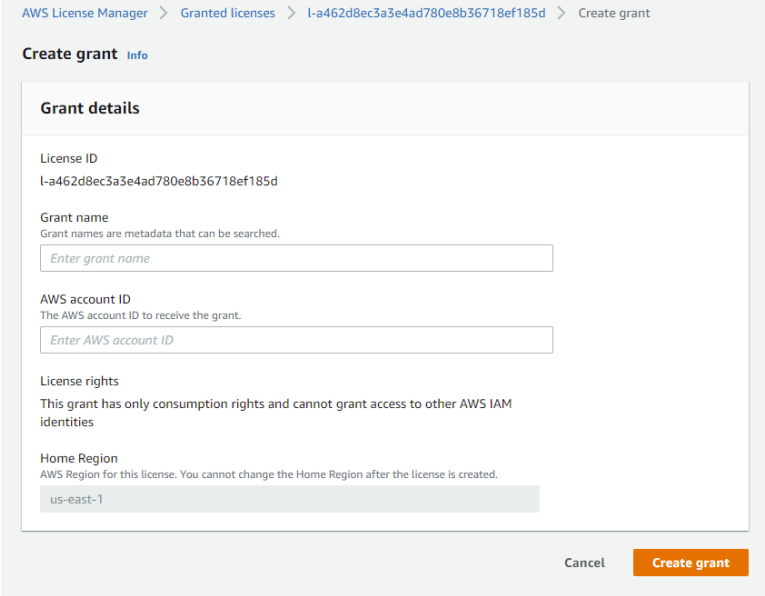


- Or you can go from the AWS Marketplace Console → Manage Subscriptions → Product detail → License hyperlink



Step 2: Create grant

- Once you click into the license details, you'll see a container labeled 'Grants'
- Click on the Create Grant button
- Populate the Grant details and the target account.



- Complete your grant distribution using the Create grant button

Grant Acceptance

- A granted license is a resource representation of the MP product subscription. Grant recipients will need to accept the license if they plan to use the license at present or in the future.
- Once a grant has been distributed to an end user account, it will show up in either Pending Acceptance or Disabled state
    - Customers using a standard billing family Org - granted licenses to an end user/recipient account will show up in a 'Pending Acceptance' state. The end user can click Accept & Activate, Accept, or Reject the License
    - Customers using All Feature Orgs - granted licenses from your management account to an end user/grantee account will automatically get accepted and show up in 'Disabled' state. The end user can Activate or Reject the license. **Note*** you must have first turned on the setting to link AWS Organizations accounts to enable the auto-acceptance functionality
- API: AcceptGrant

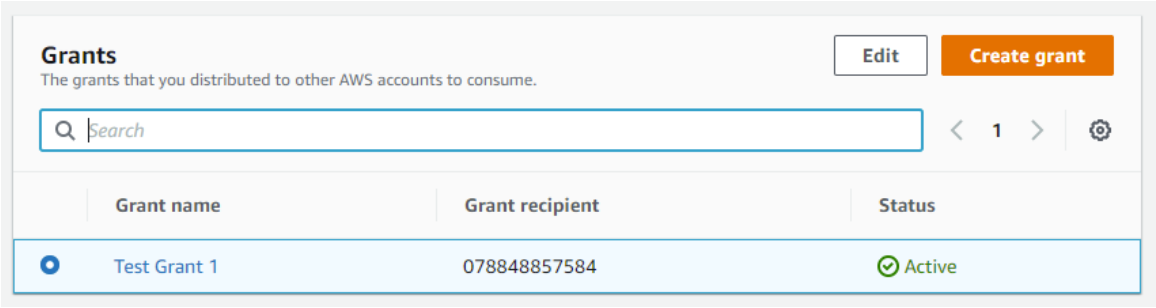
Grant Activation

- Grant activation is required for MP customers to use the license and/or spin up workloads and instances
- Once a grant has been accepted in the recipient account, it can be activated by either the Administrator or Grant recipient.
    - A Grant administrator may want to activate licenses on behalf of the recipient accounts so as to ensure end users can launch their products without the activation step
    - OR
    - A Grant recipient can choose when they want to activate it to start using the licensed product.
- API: CreateGrantVersion API set the Grant status to 'Active'

Editing Grant Name

As a grantor or administrator you may want to change or add detail to the grant name that you have already supplied.

Step 1: Find and click on the radio button next to the grant you wish to edit



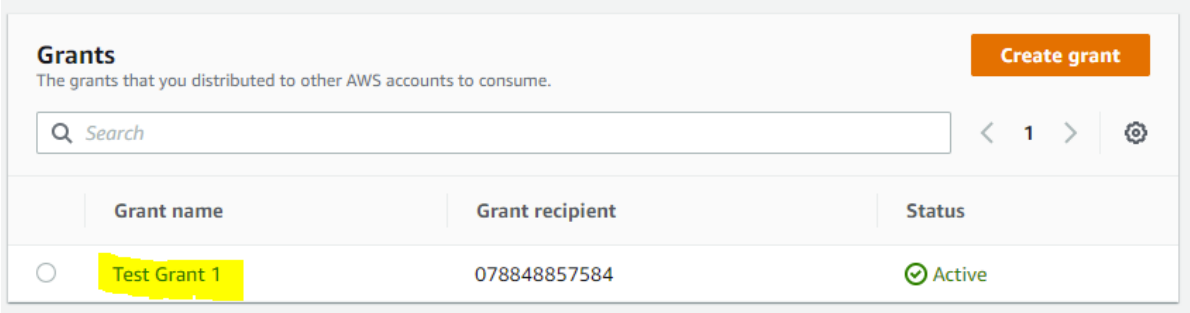
Step 2: Change or edit the grant name field

Deactivating Grants:

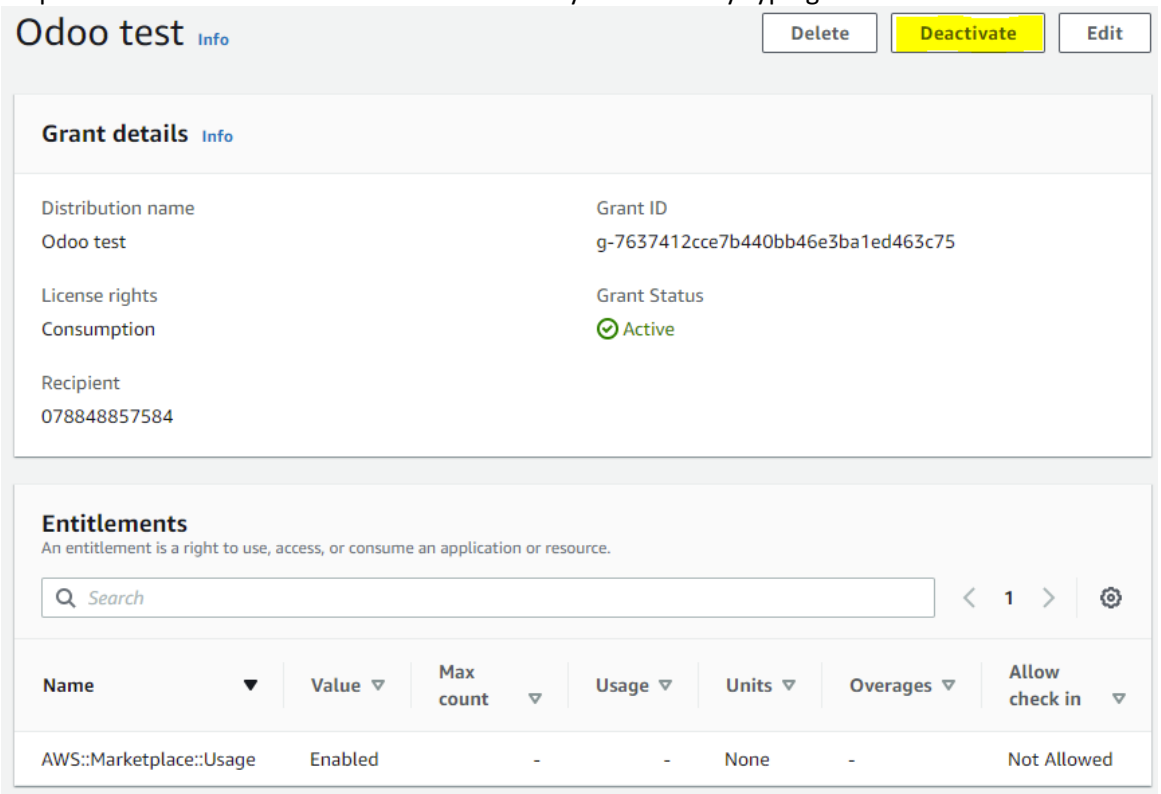
Grant recipients can deactivate their own granted licenses if they no longer want to use the license.

A grantor or administrator can also decide to deactivate the grant on behalf of the grant recipient you have previously shared the license with.

Step 1: Find and click on the grant name of the grant you wish to deactivate



Step 2: Click the deactivate button and confirm your action by typing ‘deactivate’

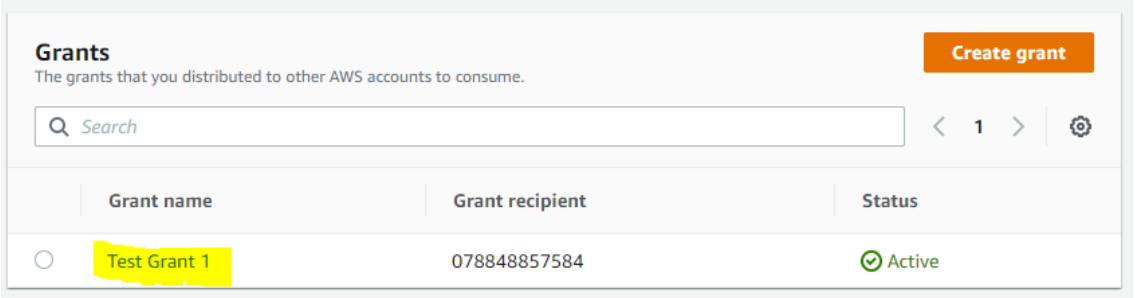


Deactivating a grant will not impact any active instances that the end user is already running from the MP product.

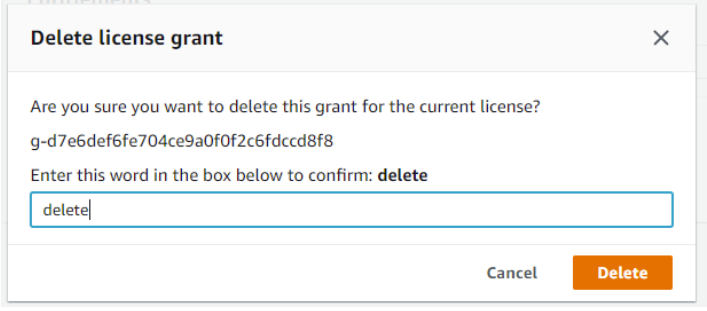
Deleting Grants:

As a grantor or administrator you can decide to stop share your MP AMI, Containers, or ML product to end users by deleting the granted license that you previously distributed.

Step 1: Find and click on the grant name of the grant you wish to delete



Step 2: Select the Delete button and confirm your deletion by typing in the word ‘delete’



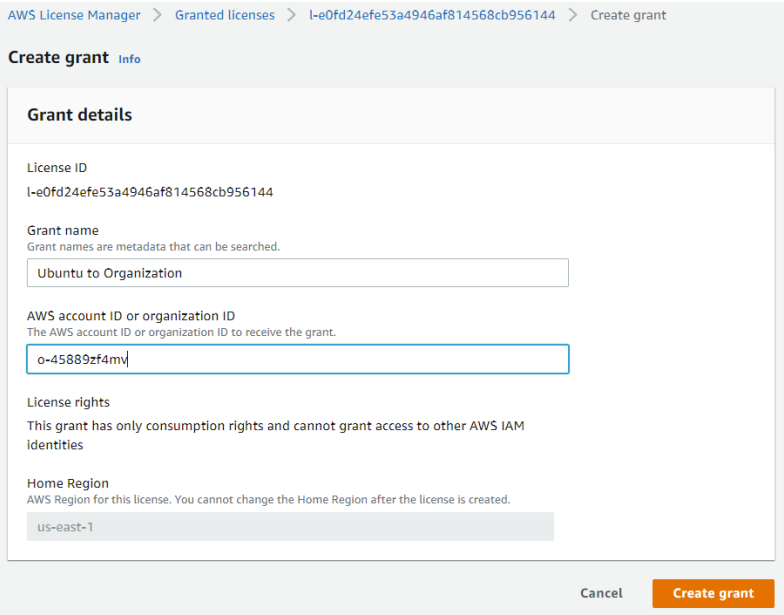
Deleting a grant will not impact any active instances that the end user is already running from the MP product. Once the grant has been deleted, the end user will no longer be able activate new instances without the granted licenses to that MP product. A deleted grant is in a terminal state, so if you have deleted a grant in error, simply recreate a new grant to the same account.

Specifying an AWS Organizations ID

Creating Grants to an AWS Organizations ID:

1. Sign in to your management account and open the AWS License Manager console.
2. To view the list of AWS Marketplace products that are already subscribed, in the navigation pane, choose **Granted Licenses.**
3. Choose the license that you want to share to your organization.
4. Choose **Create grant**.
5. On the **Create grant** page, enter values for **Grant name** and **AWS account ID or organization ID**. To get your organization ID, open the AWS Organizations console. The ID appears in the navigation pane.
6. To confirm the distribution, choose **Create grant**.

When a license is distributed to your organization, the license is automatically accepted across member accounts in the organization.

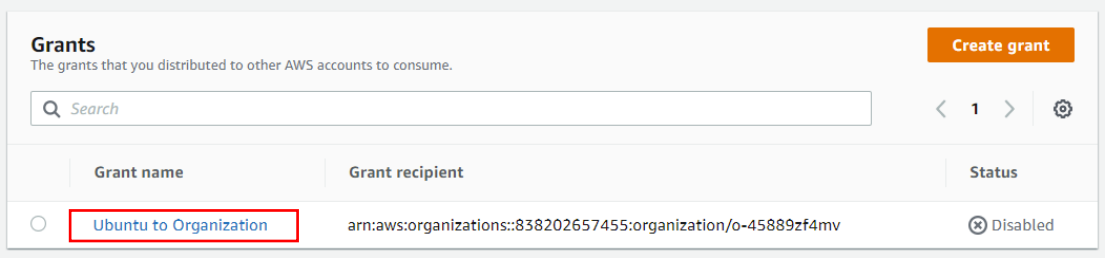


You can also create grants programmatically. For more information, see CreateGrant in the *AWS License Manager API Reference*.

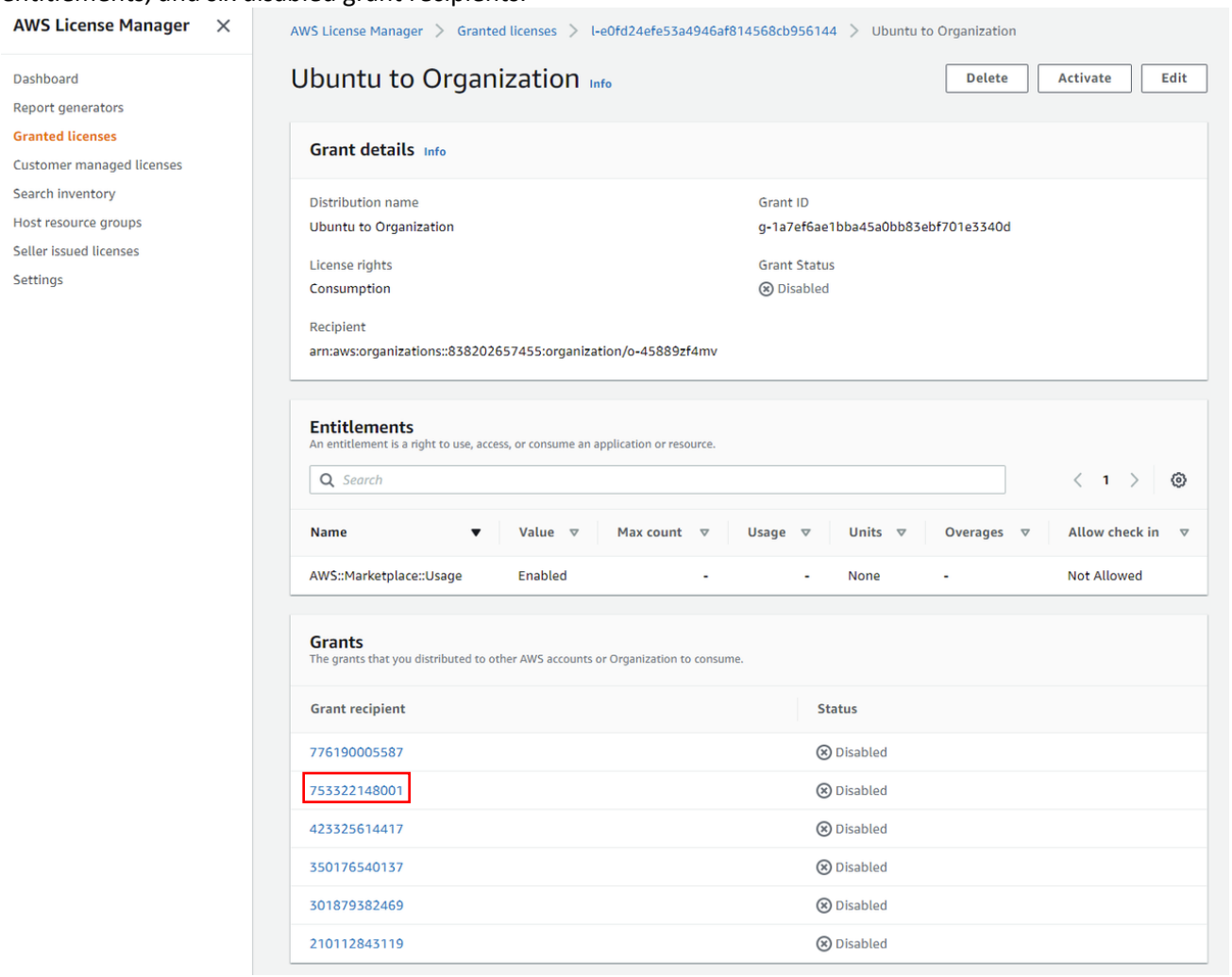
Tracking entitlements granted to your organization:

As the license grantor or administrator, you can track and manage the entitlements that you have shared across your AWS Organization at any time. To track entitlements, do the following:

1. On the AWS License Manager console, in the navigation pane, choose **Granted licenses**.
2. On the **Granted licenses** page, choose the license that you want to review.
3. On the license details page, under **Grants**, choose the grant name that corresponds to the grant that you created to your organization ID.



On the grant details page, you can view and manage your individual account-level grant statuses. The following screenshot shows my grant details page for the grant named *Ubuntu to Organization*, including grant details, entitlements, and six disabled grant recipients.



To view your distributed grants programmatically, use the ListDistributedGrants API.

Activating entitlements for your organization

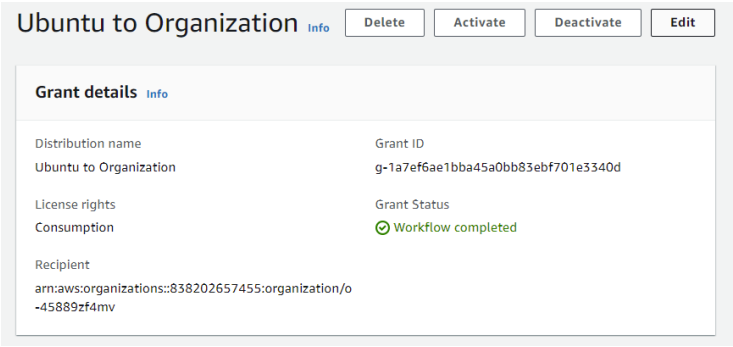
The accounts in your organization can begin using the AWS Marketplace product as soon as their granted license is activated. You can choose from multiple ways to activate a license that you granted your organization ID.

Bulk activate

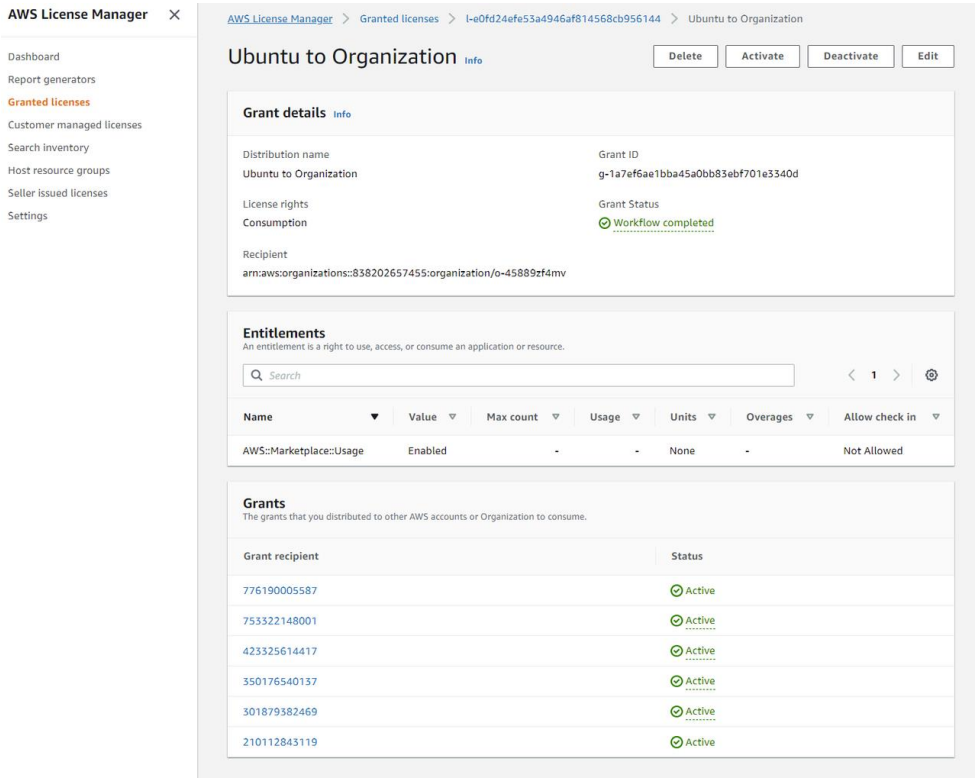
To bulk-activate all individual account licenses, do the following:

- In the AWS License Manager console, go to your organization's parent grant page and choose **Activate**.

- On the parent grant page, **Grant Status** under **Grant details** for the grant appears as **Workflow Complete** after bulk-activation and deactivation.

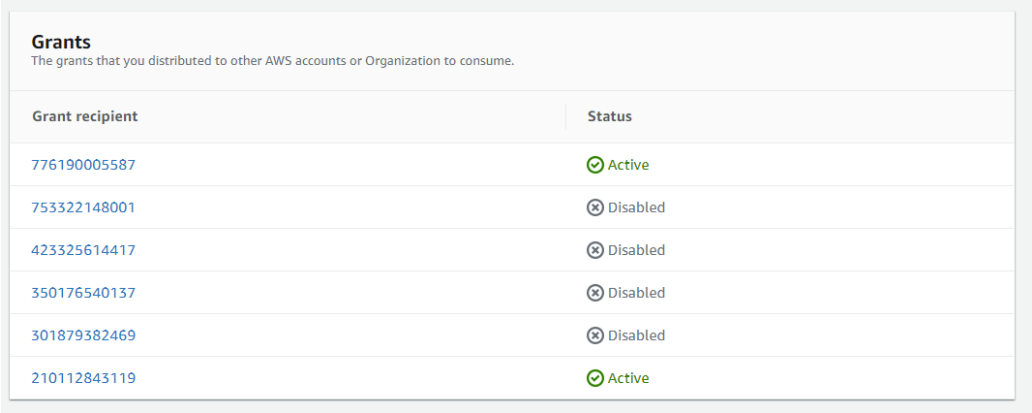


- Activation and deactivation of licenses to an organization ID triggers individual license activations at the AWS account level. In some cases, account-level licenses might not activate due to existing licenses already active in those accounts. To check account-level grant statuses, on the **Granted licenses** page, choose the name of the AWS Organizations grant to see the grant's details page.



Activate individual account grants

To activate only the grant for a specific account, in the specified license parent grant page, scroll to the **Grants** container. There, you can choose individual account grants.



Enable individual self-service activation

To have grant recipient accounts individually activate their own licenses, you can take no further action. Grant recipients can log in to AWS License Manager and activate their own licenses.

Activate grants programmatically

To activate your grants programmatically, use the CreateGrantVersion API.

Keeping track of grants to accounts in your organization

When you distribute an AWS Marketplace product license to your organization, AWS License Manager keeps track of the accounts that are being added or removed. This means that accounts being added to your organization automatically receive any licenses that are granted to the organization ID. If you previously bulk-activated all licenses across your organization, new accounts also have their licenses activated when they join. Similarly, when you remove an account from the organization, the account's distributed license is automatically disabled.

Active workloads aren't affected when a license gets disabled. Active workloads will continue to run and incur any applicable charges.

References:

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

License States

- Available: Licenses show up in Available state when it is available for use as per the terms of the MP Agreement
- Deleted: Licenses show up in Deleted state when the MP Agreement has been cancelled or terminated and the customer no longer has access to that licensed product

Grant States

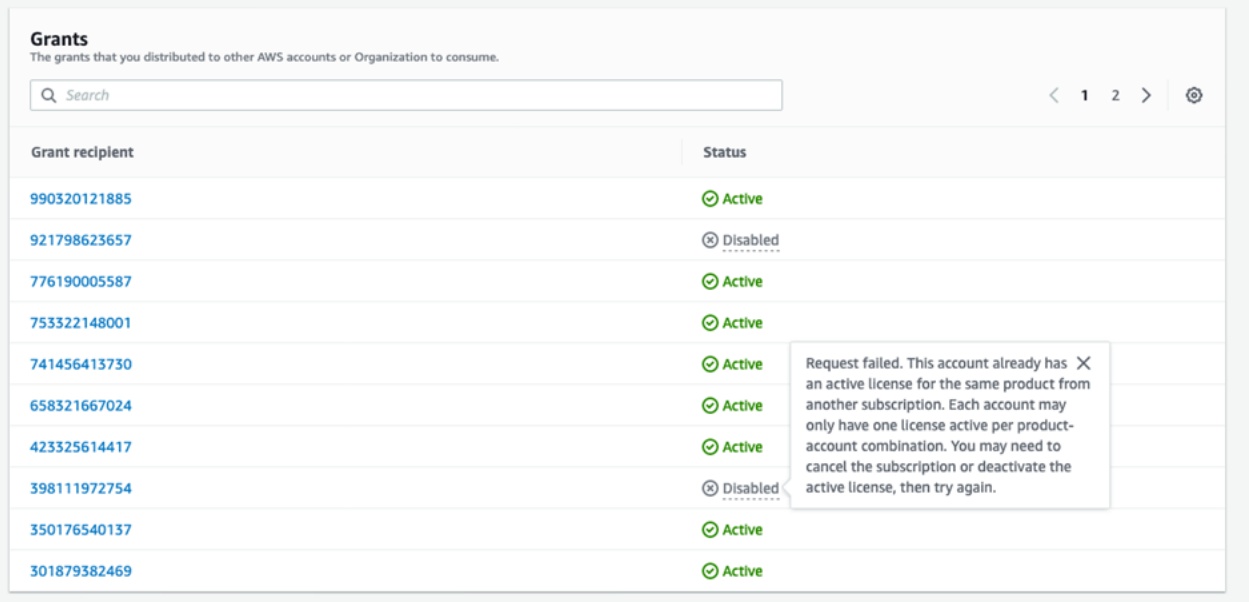
- Pending Acceptance: Grants show up in Pending Accept when the grant has been created and the grantee/end user has not yet accepted it
- Disabled: Grants show up in Disabled status when they have been accepted by the end user but not activated for immediate use
- Active: Grants show up in Active status when the end user has accepted and activated the grant successfully

- Rejected: Grants show up in Rejected status when the end user has rejected the license that was granted to them
    - Reject is a terminal state for that Grant
    - Grantor can always create a new grant for the end user on the same license
- Deleted: Grants show up in Deleted status when the grantor/administrator deletes it
    - Deleted is a terminal state for that Grant
    - Grantor can always create a new grant for the end user on the same license

Updating License status reason:

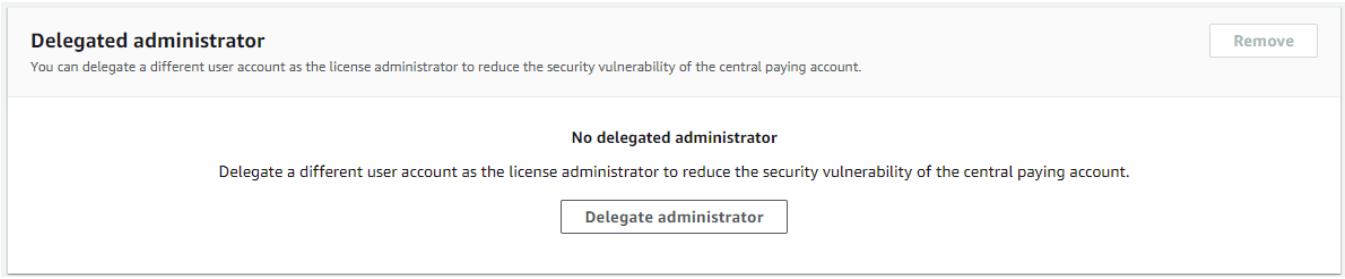
- When activating, deactivating, or deleting granted licenses, you may optionally update the license status reason via API or UI

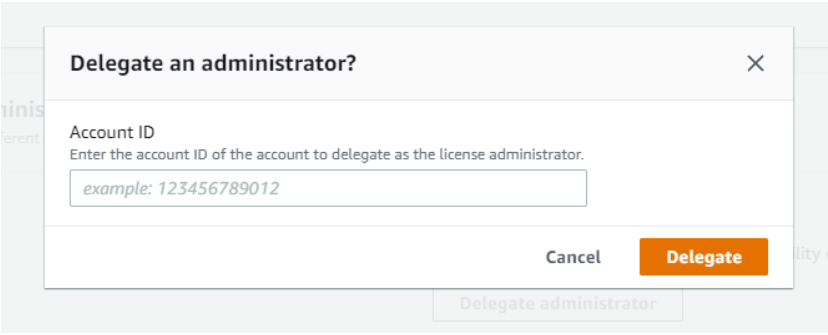
These license status updates will show up in the AWS LM Console UI, as an underlined status. These license statuses can be selected to reveal status reason messages.



Delegated Administrator for Managed entitlements – available for 'All-features' enabled organizations Delegated Administrator functionality in the AWS License Manager Service allows you to delegate a member account from your organization to perform administrative tasks such as distributing managed entitlements to other member accounts. You can register one delegated administrator account per AWS organization.

Registering your delegated administrator account: To register a delegated administrator account, log you're your Management/Payer account and navigate to the settings page in your AWS License Manager console. Select 'Delegated administrator' and type in the AWS Account ID to apply delegated administrator to the selected account. Programmatically you can also register a Delegated administrator via the RegisterDelegatedAdministrator API.





Once you have delegated an administrator account. That account can begin to manage your License Manager service activities with administrator privileges previously only given to the Management/Payer account. For managed entitlements, this means that the delegated administrator account can subscribe to AWS Marketplace products and distribute their entitlements to other members of the organization using Account ID or Org ID. Similarly, delegated administrators are who distribute entitlements can enable 'Auto-accept' granted entitlements in linked accounts and can activate distributed entitlements on behalf of linked accounts.

I have already distributed entitlements from my Management/Payer account – Can I still select a Delegated administrator?
Yes, you can add a delegated administrator even while there are existing distributed entitlements in your Management account.

Can I operate managed entitlements from my Management account and Delegated administrator account simultaneously?
Yes, AWS Marketplace subscriptions and licenses are created within the boundary of an AWS account, thus, both Management and delegated administrator accounts can distribute licenses with administrative privileges simultaneously.

I have already distributed entitlements from my Management account, can I access or manage the distribution from my newly designated Delegated Admin account?
No, each account subscribes to, and manages entitlements independently. This means that the delegated administrator account will not be able to access or manage existing licenses that are subscribed from the Management/Payer account and vice versa.

I am currently distributing entitlements from my Management account, how do I transition all entitlement distribution to my Delegated Admin account?
To transition all license distribution activities from your Management account to your delegated administrator account-- First, subscribe to the necessary products using your newly registered Delegated Administrator account. Then distribute the licenses to the necessary license recipients from your delegated administrator account. Activate the newly distributed licenses, this will automatically disable the existing distributed licenses (from the Management account) and subsequently activate the newly distributed licenses (from the Delegated Admin). This transition will not disturb any active workloads.

Once the original granted licenses are disabled, you have the option to (1) keep sharing the originally distributed entitlements from your Management account, (2) revoke the original distributed entitlements, or (3) cancel the subscription from the Management account. Keeping the original distributed entitlements shared to recipient accounts allows end users to re-activate those entitlements at any time. Revoking the original distributions prevents end users from reactivating those licenses but keeps the license subscription in the Management account for future distribution. Cancelling the subscription from the Management account will delete the product license across all recipients. To move forward with license management from the delegated administrator account, create and distribute all new MP product subscriptions using the delegated administrator account.

Once I've selected a delegated administrator account, can I unselect/remove it?
Yes, you can remove your delegated administrator account by navigating back to the AWS License Manager Console Settings page via your Management/Payer account. Alternatively, you can use the DeregisterDelegatedAdministrator API.

What happens to my distributed entitlements when the delegated administrator account is removed?
When a delegated administrator account is removed, it will no longer have governance privileges over the AWS organization, therefore there are two possible outcomes:

- If the delegated admin previously distributed license entitlements to the AWS org ID: The Org-ID distribution including granted licenses will disabled as well. This does not disrupt active workloads but will prevent license recipients from initiating new instances. Only the Management/Payer account and active Delegated Administrator account can manage license distribution via Org Id.
- If the delegated admin previously distributed license entitlements to distinct AWS Account ID(s): These distributions will remain active.

I already registered account 1234 as delegated administrator and now want to remove account 1234 and instead delegate account 4321 — Will my managed entitlements distributions from 1234 transfer to 4321?
No, each account subscribes to, and manages entitlements independently. This means that account 4321 (new) delegated administrator account will not be able to access or manage existing licenses that were subscribed from account 1234 (old) delegated admin account. New delegated admin account 4321 would subscribe/accept terms to the relevant products and distribute entitlements from their own subscription.

Frequently Asked Questions

(1) How does Managed entitlements work for MP GovCloud Customers?
Today, MP GovCloud customers have a commercial AWS account that is linked to a GovCloud account. The MP customer uses the commercial AWS account to subscribe to MP products, and through the linked relationship the GovCloud account gets automatically entitled to that subscription.

Managed entitlements operates in the same way. Managed entitlements can be performed on the commercial AWS account organization hierarchy. When a grant is distributed from a commercial management account to a commercial linked account. The GovCloud account that is tied to the commercial linked account will automatically be entitled to the MP product license. Customers can subsequently use the GovCloud account to start running the licensed software.

Note: LM Console does not yet support managed entitlements in govcloud regions, so customers will see their granted licenses in the commercial account IAD region only

(2) I have an active subscription with running instances in my linked account(s) - how do I migrate this account to a managed entitlement?

As a customer looking to transition from separate linked account subscriptions of the same product to a centrally managed subscription and granted licenses, you can easily transition your linked accounts to the centrally managed granted license.

Start with the management account of your AWS Organization, and make sure that the management account (grantor account) has subscribed to the product. Then, use AWS License Manager to grant licenses of that product to your linked accounts.

Now, the linked account will show 2 granted licenses for the same product, one as a result of their previous subscription, and the second as a result of the granted license. To migrate the linked account from their old subscription to the new granted license, simply unsubscribe from the subscription from the linked account. You can do this in the AWS Marketplace Console. Before you unsubscribe the linked account, you can choose either to keep the existing instances active, or to spin them down. Active instances will continue to be billed and charged even after the subscription is cancelled. Once the original linked account subscription is cancelled, activate the new granted license to complete the migration.

*Note that while active instances will continue to run, you will not be able to spin up any new instances until you have activated the linked account on the granted license.

Additional resources

- RIV Session: MKT204 "Who gets what? Manage software licenses across AWS accounts"
- AWS Marketplace Feature Page
- AWS License Manager Feature Page
- What's New

Blogs

- AWS News Blog/Jeff Barr Blog
- AWS Marketplace Blog
- Use managed entitlements across AWS Control Tower and AWS Service Catalog Blog
- Managed entitlements and Private Marketplace Blog
- Distribute AWS Marketplace entitlements to your organization ID
- Automating distribution of AWS Marketplace entitlements with AWS Private Marketplace and AWS Service Catalog

Documentation

- LM Granted licenses Documentation
- MP Organizational distribution Documentation
- LM API Documentation
    - CreateGrant: Creates Grant
    - AcceptGrant: Accepts Grant
    - CreateGrantVersion: Update grant to Activate Grant
    - DeleteGrants: Delete Grant
    - ListDistributedGrant: Lists distributed grants
    - GetGrant: Gets Grant Details
    - ListReceivedGrants: Lists received grants
    - RejectGrant: Rejects Grant