Getting Started Guide

AWS Partner Central

AWS Partner Central: Getting Started Guide

Table of Contents

What is AWS Partner Central?

Amazon Web Services (AWS) AWS Partner Central is an AWS service available on the AWS Management Console where AWS Partners manage their engagement with AWS.

AWS Partner Central accelerates your AWS partnership with tools, resources and APIs designed to accelerate building, marketing, and selling solutions on AWS Marketplace. With AWS Partner Central, partners can unlock benefits offered through the AWS Partner Network. To get started, sign in to the AWS console and complete registration.

For instructions to become an AWS Partner, refer to Join the AWS Partner Network.

Becoming an AWS Partner

The AWS Partner Network (APN) is a global community of partners that offers programs, expertise, and resources to build, market, and sell partner offerings. Whether you are just beginning to build or looking to expand your business, you can join the APN at no cost and use AWS trainings, enablement resources, Well-Architected tools, and more.

For instructions to become an AWS Partner, refer to Join the AWS Partner Network.

Registering in AWS Partner Central

Important

If you are an existing partner with an existing AWS Partner Central account, you should not register a new account in AWS Partner Central. Instead, the existing Alliance Lead should take the action to migrate your current AWS Partner Central account to the new experience on the AWS Console. For more information, see Migrating to Partner Central on the AWS Console.

For new sign-ups, before you can use AWS Partner Central, you must first register your company. The person who registers the company with AWS Partner Central must have the legal authority to accept the AWS Partner Central and ACE (AWS Partner Network Customer Engagements) terms and conditions on behalf of their business. During the registration process, business and identity verification processes are required.

If multiple companies, such as parent and child companies, share the same business domain and register in the AWS Partner Network, they will still share one single AWS Partner Central account.

Note

You must have an existing AWS account and proper IAM permissions before starting registration.

To register for AWS Partner Central, you'll need to sign in to the AWS Console using a designated AWS account and navigate to the AWS Partner Central service page. Before beginning the registration process, ensure you have the necessary IAM permissions in place. For more information on which AWS account to use for AWS Partner Central registration, see Linking AWS Partner Central and AWS accounts.

Note

You are not required to register in AWS Partner Central if you are only interested in selling on the AWS Marketplace and not engage in programs, funding, and co-sell with AWS. Users who register for AWS Partner Central simultaneously create Partner and Seller accounts,

and can choose to engage as a partner, seller or both. Companies can register as a Seller independent of AWS Partner Central. For more information, see Registering as a seller on AWS Marketplace.

Registration process

To register for AWS Partner Central

1. Navigate to the APN Marketing page.
2. Choose **Become a partner**. This will re-direct you to the AWS Console log in page. You must have an AWS account designated to register the AWS Partner Central service in. All AWS Partner Central users will be provisioned access to this AWS account.

   > **Important**
   >
   > You may need to reach out and request support for the following steps from your organization's IAM administrator. If you're unsure who your administrator is, you may need to reach out to your organization's IT department or whoever manages your company's AWS accounts. IAM Administrators typically sit within IT Security or Information Security departments, and sometimes in dedicated IAM teams or Governance and Compliance orgs. They should be able to direct you to the appropriate person who has administrative access to manage IAM users.

3. Identify an AWS account for AWS Partner Central. For more information on AWS account selection, see Linking AWS Partner Central and AWS accounts.
4. This IAM Administrator must provision the user performing the registration process access to the selected AWS account. This individual (the 'alliance lead') should be authorized to accept the AWS Partner Network and AWS Customer Engagement program terms and conditions on behalf of their organization, and will become the primary contact managing the AWS Partner Central account upon successful registration. For more information on what access should be provisioned, see AWS managed policies for AWS Partner Central users.
5. Once access is provisioned in IAM to the 'alliance lead', this individual should utilize their assigned IAM credentials to log into the AWS Console of the selected AWS account.
6. Choose **Sign In**. This will redirect you to the AWS Console home page.

> **Note**
>
> If your organization already has single sign-on set up to the AWS Console, you will be able to proceed with logging into the AWS account with your regular work credentials. If you do not have single sign-on enabled, enter the 12-digit AWS account ID and username and password credentials provided by your IAM administrator.

Navigate to the AWS Partner Central service page

1. Once you have successfully logged into the AWS Console home page, navigate to "AWS Partner Central" by using the console navigation or using the console search.
2. Choose AWS Partner Central to go to the AWS Partner Central service page and choose **Get started**.

> **Important**
>
> If you are unable to complete the registration process and require support, contact APN Support Team through this external link.

Complete the business and identity verification processes

AWS Partner Central requires new partners to complete both identity verification and business verification processes during registration. These verification steps validate individual identities and business credentials through government and public data sources.

To complete verification

1. Choose **Get Started** to begin the registration process.
2. A modal will appear on the screen. Review the pre-registration requirements to ensure you have all required materials before proceeding.

> **Important**
>
> The identity verification process requires you to upload a selfie and picture of a government ID. Ensure you have adequate lighting and a stable internet connection. Each QR code is session-specific.

3. Choose **Continue to Registration** to proceed to the verification process.
4. The system will display a unique QR code for mobile verification.
5. Use your mobile device to scan the QR code displayed on your computer screen. This will re-direct you to a mobile verification flow.
6. Complete the identity verification workflow from your mobile device.
7. Choose **Next** to submit your verification. Identity Verification typically takes under a minute to complete. Upon successful verification of identity, your Verification Status will show as 'Complete'.

> **Note**
>
> If verification fails, click **Refresh** to generate a new QR code. Repeat the mobile verification process. Ensure good lighting and image quality. You can attempt identity verification three times within a 24-hour period. If you fail three times, you can retry after 24 hours.

8. Choose **Next** to continue to the business verification process.

> **Important**
>
> Identity verification must be completed successfully before starting business verification. Ensure you have your company's legal name and tax ID before continuing.

9. Complete the business verification fields. If you use and have permissions for the Tax Console already, your business information will be pre-populated. If not, enter the corresponding data, including: Legal business name (as registered), Country of incorporation, Tax ID or Business Registration Number, and State or Province.
10. Review all entered information for accuracy before final submission. Once completed, select **Next** to begin business verification.

> **Note**
>
> This process can take up to an hour. You can stay on this page or leave and return later. If your business verification failed, select **Re-try** and complete the form, ensuring accurate information.

11. Once your business is verified successfully, you will see a green success bar at the top of the page. Select **Continue Registration** to proceed.

> **Important**
>
> If you are unable to complete the registration process and require support, contact APN Support Team through this external link.

Complete registration form

To complete registration

1. Enter contact information for the Alliance Lead. This should be your organization's primary contact. All AWS Partner Network communications and key updates, such as the APN Newsletter or email announcements about changes in policies or new feature launches, will only be sent to this primary contact.

   > **Important**
   >
   > For organizations who wish to distribute communications to a wider audience, we recommend using a shared email alias as the primary contact, which allows communication to go to all individuals with access to that shared inbox.

2. Provide basic details about your organization, including your primary product or service and industry focus.
3. Choose **Next**. Review information and prepare to complete registration. Choose **Edit** for the corresponding section if any updates are required.
4. Add tags (optional). Tags allow partners to label specific resources (such as Opportunities or Fund Requests) and control access based on these tags. For example, partners can tag

opportunities by Region or Sector and restrict individual user access to these specific segments of their AWS Partner Central data.

5. Review the Terms and Conditions.
6. Choose **Submit Registration**.

> **Note**
>
> Separate AWS Partner Central and Marketplace accounts are created at the time of registration. Partners do not need to register as a Seller on the AWS Marketplace unless they choose to. The system automatically creates both accounts to ensure partners have access to all potential opportunities, even if not immediately needed.

7. Choose **Continue to AWS Partner Central** and begin completing onboarding tasks to get started.

Registration FAQs

Our organization has multiple AWS account IDs. How do I know which AWS account ID to use?

Use an AWS account that can serve as the primary account for managing AWS-related partnership activities. All AWS Partner Central users will be provisioned access to the AWS account. AWS recommends not using a Management/Payer account but instead setting up a Member account within your AWS Organizations structure. Contact your organization's IAM Administrator if unsure of which AWS account to use, or if a new AWS account must be created.

How do I know if my company has a AWS Partner Central account?

During the registration process, your registration business validation will fail if a company with the same Legal business name and details exists in our database. Contact Partner Central Support if you need to merge or consolidate APN accounts.

How do I know if I am a root user?

You are a root user if you created the AWS account and sign in using the email address and password used to create the account, rather than IAM credentials. AWS recommends not logging in as a root user. More information can be found here.

Can the alliance lead contact information be updated after registering?

Yes, the alliance lead contact information can be updated at any time. For more information, see Partner Central settings.

Who should complete the identity verification process?

An individual authorized to register a AWS Partner Central account can complete this.

What are you doing with the identity verification data?

The data is used to verify identity, establish partner credentials, and maintain partner program compliance.

What happens if I register the AWS Partner Central Account and then change roles or leave my company? What happens to my personal data?

Your organization's account administrator can transfer account management to another person. Personal data acquired in registration can be updated or removed upon request through AWS Partner Support.

Are all international IDs valid?

AWS accepts most government-issued IDs, but some restrictions may apply based on country-specific regulations.

How do I cancel?

Contact Partner Central Support to deactivate an existing account.

Why does my account summary on the dashboard of AWS Partner Central show "Not Registered" even though I've already registered with the APN?

If you have an AWS Marketplace account and see a "Not Registered" message in AWS Partner Central in the Console, this means you haven't completed your migration from the legacy Partner Central experience.

> **Important**
>
> Do not create a new profile or register again. Creating a new registration will replace all of your historical partner data.

What should I do? Work with your IT administrator to schedule your migration from legacy Partner Central to the new AWS Partner Central in the Console. This will preserve all of your existing partner history and data.

User management

User access to AWS Partner Central is managed through AWS Identity and Access Management (IAM). The below topics describe how to invite, onboard, manage and troubleshoot permissions for AWS Partner Central users.

Topics

Controlling access in AWS Partner Central

User access to AWS Partner Central is managed through AWS Identity and Access Management (IAM). IAM permissions control who can be authenticated (signed in) and authorized (have permissions) to use AWS Partner Central and AWS Marketplace features. IAM is an AWS service that you can use at no additional charge.

IAM permissions are assigned to individual users by IAM Administrators. These administrators act as security managers for your AWS environment—they provision and de-provision user accounts, assign permissions, and set up security policies. IAM Administrators typically sit within IT or Governance and Security teams.

> **Important**
>
> To access AWS Partner Central, users must work with their IAM Administrator to be provided with the correct level of access. If permissions aren't set up correctly, users might not be able to sign in at all, or they might be able to log in, but may not be able to access the tools and information they need to do their job.

The following resources provide more information about getting started and using IAM:

- Create an administrative user

- Security best practices in IAM
- Managing IAM policies
- Attaching a policy to an IAM user group
- IAM Identities (users, groups, and roles)
- Controlling access to AWS resources using policies
- Actions, resources, and condition keys for AWS services

Topics

AWS IAM for AWS Partner Central

AWS IAM is built on the concept of role-based access. Within this framework, users are assigned to specific roles or groups associated with a set of IAM policies that control what specific features within AWS Partner Central that a user can access. To simplify this process, AWS has published several Managed policies to simplify user management for common user personas within AWS Partner Central.

The IAM Administrator is responsible for the creation of IAM roles, groups and policies and assignment of users to provision permissions in AWS IAM, but must collaborate with the Partner Central users and their leadership to determine what level of access each user should be granted.

Review the Managed policy mappings for guidance on managed policy assignments based on common Partner Central user personas.

Working with AWS IAM requires specific technical knowledge and appropriate AWS account permissions. These individuals ('IAM Administrators') are required to support set up and management of these permissions. The IAM Administrator is typically someone in your IT Security, Information Security, or Governance/Compliance department.

Partner Central uses AWS IAM to manage all user access through your organization's AWS account. Instead of Partner Central managing users directly, your IT team controls access through AWS IAM. Users are assigned specific policies that determine which Partner Central resources (like

Opportunities, Solutions, or Fund Requests) a user can access and whether they can only view information (read access) or also make changes (write access).

> **Important**
>
> If users are not properly provisioned access in IAM, they will not be able to access features in AWS Partner Central. Users should only have access to the features they need to do their job - this is called "least privilege" access.

IAM Role-Based Access Implementation

Implementation varies by organization but generally follows this process:

Step 1: The IAM Administrator creates IAM roles

IAM Administrators create roles that define functional personas within AWS Partner Central. Each role describes the specific features and capabilities users in that job function need to access. For example, a role could be created for:

- Marketing Managers, responsible for creating co-marketing assets and managing campaigns
- Operations Administrators, responsible for creating and managing fund requests.

Organizations can create as many roles as needed based on the different personas accessing Partner Central. For a summary of common Partner Central user personas, see here. In addition to these managed policies, organizations can create and customize managed policies to tailor access as needed. For more information, see AWS managed policies for AWS Partner Central users.

> **Note**
>
> Not sure who your IAM Administrator is? They typically sit in IT Security, Information Security, or Governance/Compliance teams, but this varies by organization. They should have administrator access to the AWS account used to access AWS Partner Central.

Step 2: Assign IAM Policies to Each Role

Once roles are created, the IAM Administrator assigns specific IAM policies that determine allowed access. For example, the Marketing Manager role might receive read/write access to

the Case Studies feature, permission to create and manage Solutions, and the ability to create tickets to APN Support. To simplify this process, AWS publishes Managed Policies—pre-built sets of IAM policies that map to common user roles. Instead of provisioning individual feature-level inline policies, IAM Administrators can assign Managed Policies that align with each role's responsibilities. To see how common Partner Central personas map to published Managed Policies, see here.

> **Note**
>
> IAM Administrators can use managed policies or build custom policies for specific user permissions. AWS recommends using managed policies when possible to simplify permission management, as they enable automatic AWS updates for common use cases and version control.

Step 3: [Optional] Set up Single Sign-On

Single Sign-On (SSO) benefits users, organizations, and IT teams by streamlining authentication and enhancing security. For users, SSO simplifies access by allowing them to log in once, with a single set of credentials, to access multiple enterprise applications, reducing password fatigue and enabling faster productivity through seamless navigation across integrated systems. For organizations, SSO enhances security through centralized authentication that enables stronger access controls and improves compliance by making it easier to enforce security policies. For IT teams specifically, SSO simplifies administration by managing user identities and permissions from a single location, accelerates onboarding and offboarding by granting or revoking access to multiple systems simultaneously, and offers integration flexibility by connecting diverse applications through standard protocols. For more information on how to set up SSO for your organization, see here.

Adding users to AWS Partner Central

Adding users to Partner Central requires coordination between the Alliance Lead (who determines access needs) and the IAM Administrator (who implements the technical setup).

> **Note**
>
> IAM permissions can be modified whenever needed, and there's no cap on how many users can receive access rights.

To add a new user:

For Alliance Leads: Determine User Access Needs

1. **Identify the user's role and required access level:** Review the managed policy mappings to determine which role (persona) best describes their job function. Refer to this table for common Partner Central user personas and which Managed policies best fit that user's required level of access.
2. **Request the IAM Administrator to add the user.** Provide the IAM Administrator with:
   - User's name and company email address
   - Required managed policies (e.g., AWSPartnerCentralOpportunityManagement)
   - Any specific access requirements if custom policies are needed

For IAM Administrators: Create and Configure User Access

Depending on your AWS account setup, choose one of the following options to grant users access:

Option 1: Using IAM Identity Center

Best for: Organizations managing multiple users across AWS accounts who want centralized access management with single sign-on (SSO) capabilities.

Key benefits: Centralized user management, automatic permission synchronization across accounts, simplified onboarding/offboarding, and enhanced security with SSO.

Option 2: Using IAM Console (For individual users)

Best for: Small teams or organizations managing a limited number of individual user accounts who need direct AWS Console access.

Key benefits: Quick setup for individual users, direct control over specific user permissions, and straightforward for small-scale deployments.

Option 3: Integrate with a third-party Identity Provider

Best for: Organizations already using enterprise identity providers (like Okta, Azure AD, or Ping Identity) who want to maintain existing authentication workflows.

Key benefits: Seamless integration with existing enterprise identity systems, consistent authentication experience across all business applications, centralized user lifecycle management, and enhanced compliance with corporate security policies.

Permissions for AWS Partner Central

You can use the following permissions in IAM policies for AWS Partner Central. You can combine permissions into a single IAM policy to grant the permissions you want.

ListPartnerPaths

`ListPartnerPaths` provides access to list partner paths in AWS Partner Central.

- **Action groups:** `ListOnly`, `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

EnrollInPartnerPath

`EnrollInPartnerPath` provides access to enroll in partner paths in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

GetPartnerDashboard

`GetPartnerDashboard` provides access to retrieve partner dashboard information in AWS Partner Central.

- **Action groups:** `ReadOnly`, `ReadWrite`

- **Required resources:** `arn:${Partition}:partnercentral::${Account}:catalog/${Catalog}/ReportingData/${TableId}/Dashboard/${DashboardId}`
- **Condition keys:** `partnercentral:Catalog`

CreateBusinessPlan

`CreateBusinessPlan` provides access to create business plans in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

PutBusinessPlan

`PutBusinessPlan` provides access to update business plans in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

ListBusinessPlans

`ListBusinessPlans` provides access to list business plans in AWS Partner Central.

- **Action groups:** `ListOnly`, `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

GetBusinessPlan

`GetBusinessPlan` provides access to retrieve business plan details in AWS Partner Central.

- **Action groups:** `ReadOnly`, `ReadWrite`

- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

CreateCollaborationChannelRequest

`CreateCollaborationChannelRequest` provides access to create collaboration channel requests in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

ListCollaborationChannels

`ListCollaborationChannels` provides access to list collaboration channels in AWS Partner Central.

- **Action groups:** `ListOnly`, `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

GetCollaborationChannel

`GetCollaborationChannel` provides access to retrieve collaboration channel details in AWS Partner Central.

- **Action groups:** `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

CreateCollaborationChannelMembers

`CreateCollaborationChannelMembers` provides access to create collaboration channel members in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

SearchPartnerProfiles

`SearchPartnerProfiles` provides access to search public partner profiles in AWS Partner Central.

- **Action groups:** `ListOnly`, `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

GetPartnerProfile

`GetPartnerProfile` provides access to retrieve public partner profile details in AWS Partner Central.

- **Action groups:** `ReadOnly`, `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

GetProgramManagementAccount

`GetProgramManagementAccount` provides access to retrieve program management account details in AWS Partner Central.

- **Action groups:** `ReadOnly`, `ReadWrite`

- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.
- **Condition keys:** `partnercentral:Catalog`

UseSession

`UseSession` provides access to use Partner Central agents sessions in AWS Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.
- **Condition keys:** `partnercentral:Catalog`

Condition keys for AWS Partner Central

AWS Partner Central defines the following condition keys that you can use in the `Condition` element of an IAM policy.

partnercentral:Catalog

Filters access by a specific Catalog.

- **Type:** `String`

  Valid values: `[AWS | Sandbox]`

partnercentral:RelatedEntityType

Filters access by entity types for Opportunity association.

- **Type:** `String`

  Valid values: `[Solutions | AwsProducts | AwsMarketplaceOffers]`

partnercentral:ChannelHandshakeType

Filters access by channel handshake types.

- **Type:** `String`

  Valid values: `[START_SERVICE_PERIOD | REVOKE_SERVICE_PERIOD | PROGRAM_MANAGEMENT_ACCOUNT]`

partnercentral:VerificationType

Filters access by the type of verification being performed.

- **Type:** `String`

  Valid values: `[BUSINESS_VERIFICATION | REGISTRANT_VERIFICATION]`

partnercentral:FulfillmentTypes

Filters access by benefit fulfillment types.

- **Type:** `ArrayOfString`

  Valid values: `[CREDITS | CASH | ACCESS]`

partnercentral:Programs

Filters access by program.

- **Type:** `ArrayOfString`

Controlling access in AWS Partner Central account management

AWS Identity and Access Management (IAM) is an AWS service you can use at no additional charge that helps you control access to AWS resources. AWS Partner Central account management uses IAM for AWS Partner Central authentication and authorization. Administrators can use IAM roles

to control who can sign in to AWS Partner Central and what AWS Partner Central permissions they have.

> **Important**
>
> AWS Partner Central users that you create authenticate using their credentials. However, they must use the same AWS account. Any change a user makes can impact the entire account.

For more information about available actions, resources, and condition keys, refer to Actions, resources, and condition keys for AWS services.

Topics

Permissions for AWS Partner Central account management

You can use the following permissions in IAM policies for AWS Partner Central account management. You can combine permissions into a single IAM policy to grant the permissions you want.

AssociatePartnerAccount

`AssociatePartnerAccount` provides access to associate AWS Partner Central and AWS accounts.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

AssociatePartnerUser

`AssociatePartnerUser` provides access to associate AWS Partner Central users and IAM roles.

- **Action groups:** `ReadWrite`

- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

DisassociatePartnerUser

`DisassociatePartnerUser` provides access to associate AWS Partner Central users and IAM roles.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.

AccessLegacyPartnerCentral

`AccessLegacyPartnerCentral` provides access to Single Sign-On from AWS Partner Central into Legacy Partner Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.
- **Condition keys:** `partnercentral-account-management:LegacyPartnerCentralRole`

AccessMarketingCentral

`AccessMarketingCentral` provides access to Single Sign-On from AWS Partner Central into Marketing Central.

- **Action groups:** `ReadWrite`
- **Required resources:** Does not support specifying a resource Amazon Resource Number (ARN) in the `Resource` element of an IAM policy statement. To allow access, specify `"Resource": "*"` in your policy.
- **Condition keys:** `partnercentral-account-management:MarketingCentralRole`

Condition keys for AWS Partner Central account management

AWS Partner Central account management defines the following condition keys that you can use in the `Condition` element of an IAM policy.

partnercentral-account-management:LegacyPartnerCentralRole

Filters access by the Legacy Partner Central role. Accepted values: [AceManager, TechnicalStaff, ChannelUser, MarketingStaff].

- **Type:** `ArrayOfString`

partnercentral-account-management:MarketingCentralRole

Filters access by Marketing Central role. Accepted values: [portal-manager, marketing-staff, sales-representative].

- **Type:** `ArrayOfString`

Additional resources

Refer to the following sections of the IAM User Guide for more information:

- Security best practices in IAM
- Managing IAM policies
- Attaching a policy to an IAM user group
- IAM identities (users, user groups, and roles)
- Controlling access to AWS resources using policies

AWS managed policies for AWS Partner Central users

An AWS managed policy is a standalone policy created and administered by AWS. AWS managed policies provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies specific to your use cases. For more information, refer to AWS managed policies.

The AWS managed policies described in this section manage AWS Partner Central users' access to AWS Marketplace. For more information about AWS Marketplace seller policies, refer to AWS managed policies for AWS Marketplace sellers.

Topics

AWS managed policy: `AWSPartnerCentralFullAccess`

You can attach the `AWSPartnerCentralFullAccess` policy to your IAM identities.

This policy grants full access to AWS Partner Central and related AWS services.

To view the permissions for this policy, see AWSPartnerCentralFullAccess in the *AWS Managed Policy Reference*.

AWS managed policy: `PartnerCentralAccountManagementUserRoleAssociation`

You can attach the `PartnerCentralAccountManagementUserRoleAssociation` policy to your IAM identities. This policy is used by a partner cloud admin to manage IAM roles linked to partner users.

This policy allows the following operations:

- List all roles.
- Pass an IAM role with the name prefix `PartnerCentralRoleFor` to the AWS Partner Central account management service.
- Associate a AWS Partner Central user with an IAM role.
- Disassociate a AWS Partner Central user from an IAM role.

To view the permissions for this policy, see PartnerCentralAccountManagementUserRoleAssociation in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralOpportunityManagement

You can attach the `AWSPartnerCentralOpportunityManagement` policy to your IAM identities.

This policy grants full access to manage opportunities in AWS Partner Central.

To view the permissions for this policy, see AWSPartnerCentralOpportunityManagement in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralSandboxFullAccess

You can attach the `AWSPartnerCentralSandboxFullAccess` policy to your IAM identities.

This policy grants access for developer testing in the Sandbox catalog.

To view the permissions for this policy, see AWSPartnerCentralSandboxFullAccess in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePoli

You can attach the `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` policy to your IAM identities.

This policy provides the ResourceSnapshotJob with permission to read a resource and snapshot it in the target environment. For more information on how to use this policy, see Working with multi-partner opportunities in the *AWS Partner Central API Reference*.

To view the permissions for this policy, see AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralChannelManagement

You can attach the `AWSPartnerCentralChannelManagement` policy to your IAM identities.

This policy grants access to manage channel programs and relationships in AWS Partner Central.

To view the permissions for this policy, see AWSPartnerCentralChannelManagement in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralChannelHandshakeApprovalManagement

You can attach the `AWSPartnerCentralChannelHandshakeApprovalManagement` policy to your IAM identities.

This policy grants access to channel handshake approval management activities in AWS Partner Central.

To view the permissions for this policy, see AWSPartnerCentralChannelHandshakeApprovalManagement in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerCentralMarketingManagement

You can attach the `AWSPartnerCentralMarketingManagement` policy to your IAM identities.

This policy grants access to manage marketing activities and campaigns in AWS Partner Central.

To view the permissions for this policy, see AWSPartnerCentralMarketingManagement in the *AWS Managed Policy Reference*.

AWS managed policy: PartnerCentralIncentiveBenefitManagement

You can attach the `PartnerCentralIncentiveBenefitManagement` policy to your IAM identities.

This policy grants access to manage all the incentive benefits in AWS Partner Central.

To view the permissions for this policy, see PartnerCentralIncentiveBenefitManagement in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerProServeToolsFullAccess

You can attach the `AWSPartnerProServeToolsFullAccess` policy to your IAM identities.

This policy grants full access to AWS ProServe Tools (A2T and MPA) via AWS Partner Central Single Sign-On. It includes all assessment roles — individual contributor, organization reader, organization contributor, and organization admin — enabling complete access to create, read, update, and share assessments across the organization, as well as manage organization-level settings.

Roles granted:

- AssessmentIndividualContributor
- AssessmentOrganizationReader
- AssessmentOrganizationContributor
- OrganizationAdmin

To view the permissions for this policy, see AWSPartnerProServeToolsFullAccess in the *AWS Managed Policy Reference*.

AWS managed policy: AWSPartnerProServeToolsOrganizationReaderIndividualContribut

You can attach the `AWSPartnerProServeToolsOrganizationReaderIndividualContributor` policy to your IAM identities.

This policy grants read access to all organizational assessments in A2T, combined with the ability to create and manage the user's own assessments in both A2T and MPA. It is intended for users who need visibility into team assessments while retaining the ability to manage their own work.

> **Note**
>
> MPA does not support read-only mode. Users assigned this policy will retain read/write access to their own MPA assessments.

Roles granted:

- AssessmentIndividualContributor
- AssessmentOrganizationReader

To view the permissions for this policy, see AWSPartnerProServeToolsOrganizationReaderIndividualContributor in the *AWS Managed Policy Reference*.

AWS managed policy: `AWSPartnerProServeToolsIndividualContributor`

You can attach the `AWSPartnerProServeToolsIndividualContributor` policy to your IAM identities.

This policy grants the minimum permissions required to access AWS ProServe Tools via AWS Partner Central Single Sign-On. Users can create, read, update, and share their own assessments in both A2T and MPA. Access is scoped to assessments created by the user's own IAM identity (role or user ARN).

Roles granted:

- AssessmentIndividualContributor

To view the permissions for this policy, see AWSPartnerProServeToolsIndividualContributor in the *AWS Managed Policy Reference*.

AWS Partner Central updates to AWS managed policies

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

Change	Description	Date
AWSPartnerProServeToolsFullAccess — New policy	AWS Partner Central added a new policy to grant full access	March 23, 2026

Change	Description	Date
	to AWS ProServe Tools (A2T and MPA) via AWS Partner Central Single Sign-On with all assessment roles.	
AWSPartnerProServeToolsOrganizationReaderIndividualContributor — New policy	AWS Partner Central added a new policy to grant read access to organizational assessments in A2T and manage own assessments in both A2T and MPA.	March 23, 2026
AWSPartnerProServeToolsIndividualContributor — New policy	AWS Partner Central added a new policy to grant minimum permissions to access AWS ProServe Tools and manage own assessments.	March 23, 2026
PartnerCentralIncentiveBenefitManagement — Update to an existing policy	AWS Partner Central updated a policy to add Partner Central Agents session management capability through the Model Context Protocol.	March 13, 2026
AWSPartnerCentralOpportunityManagement — Update to an existing policy	AWS Partner Central updated a policy to add Partner Central Agents session management capability through the Model Context Protocol.	March 13, 2026

Change	Description	Date
AWSPartnerCentralSandboxFullAccess — Update to an existing policy	AWS Partner Central updated a policy to add Partner Central Agents session management capability through the Model Context Protocol.	March 13, 2026
AWSPartnerCentralFullAccess — Update to an existing policy	AWS Partner Central updated a policy to add Partner Central Agents session management capability through the Model Context Protocol.	March 13, 2026
AWSPartnerCentralOpportunityManagement — Update to an existing policy	AWS Partner Central updated a policy to add Amazon Q permissions for Partner Assistant chatbot functionality.	February 23, 2026
AWSPartnerCentralChannelManagement — Update to an existing policy	AWS Partner Central updated a policy to add Amazon Q permissions for Partner Assistant chatbot functionality.	February 23, 2026
AWSPartnerCentralMarketingManagement — Update to an existing policy	AWS Partner Central updated a policy to add Amazon Q permissions for Partner Assistant chatbot functionality.	February 23, 2026
PartnerCentralIncentiveBenefitManagement — New policy	AWS Partner Central added a new policy to grant access to all the incentive benefits functionality.	February 11, 2026

Change	Description	Date
AWSPartnerCentralFullAccess — Update to an existing policy	AWS Partner Central updated a policy to add Amazon Q permissions for Partner Assistant chatbot functionality and to add AWS Marketplace Agreements read access for MPOPP benefits functionality.	February 4, 2026
AWSPartnerCentralMarketingManagement — New policy	AWS Partner Central added a new policy to grant access to manage partner central marketing and campaigns.	November 30, 2025
AWSPartnerCentralFullAccess — Update to an existing policy	AWS Partner Central updated a policy to add legacy Partner Central access, put files into S3, and get AWS Marketplace entities.	November 30, 2025
AWSPartnerCentralOpportunityManagement — Update to an existing policy	AWS Partner Central updated a policy to add engagement context access, opportunity from engagement task access, and legacy Partner Central access, get dashboard, collaboration channel access, get partner, and tag opportunity and resource snapshot jobs.	November 30, 2025
AWSPartnerCentralChannelManagement — Update to an existing policy	AWS Partner Central updated a policy to add legacy Partner Central access, get dashboard, and get partner.	November 30, 2025

Change	Description	Date
AWSPartnerCentralFullAccess — Update to an existing policy	AWS Partner Central updated a policy to add Channel billing transfer role access.	November 19, 2025
AWSPartnerCentralChannelManagement — New policy	AWS Partner Central added a new policy to grant access to manage channel management activities.	November 19, 2025
AWSPartnerCentralChannelHandshakeApprovalManagement — New policy	AWS Partner Central added a new policy to grant access to channel handshake approval management activities.	November 19, 2025
AWSPartnerCentralFullAccess — Update to an existing policy	AWS Partner Central updated a policy.	December 4, 2024
AWSPartnerCentralOpportunityManagement — Update to an existing policy	AWS Partner Central updated a policy.	December 4, 2024
AWSPartnerCentralSandboxFullAccess — Update to an existing policy	AWS Partner Central updated a policy.	December 4, 2024
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy — New policy	AWS Partner Central added a new policy to grant access to read resources and create snapshots.	December 4, 2024
AWSPartnerCentralFullAccess – New policy	AWS Partner Central added a new policy to grant full access to the AWS Partner Central service.	November 18, 2024

Change	Description	Date
AWSPartnerCentralOpportunityManagement — New policy	AWS Partner Central added a new policy to grant full access to manage opportunities in AWS Partner Central.	November 14, 2024
AWSPartnerCentralSandboxFullAccess — New policy	AWS Partner Central added a new policy to grant access for developer testing in the Sandbox catalog.	November 14, 2024
AWS Partner Central started tracking changes	AWS Partner Central started tracking changes for its AWS managed policies.	November 14, 2024

Mapping Partner Central Users to Managed Policies

Understanding Partner Central Personas and Policy Mapping

Each persona represents a distinct role within your partner organization with specific access needs to AWS Partner Central features. Match your users to these personas to assign the appropriate managed policy that grants necessary permissions while maintaining security best practices.

> **Important**
>
> All managed policies below grant users access to Amazon Q, an AI-powered assistant providing real-time support and guidance within AWS Partner Central. For more information on Amazon Q, see here.

Common AWS Partner Central User Personas

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
IAM Administrator	This individual typically sits in IT Security, Information Security, or Governance/Compliance teams, but this varies by organization. They should have administrator access to the AWS account used to access AWS Partner Central.	This individual should have administrator rights within the AWS account in order to provision users' IAM permissions	• Collaborate with alliance lead/users to understand level of access required • Onboard users to AWS IAM and provision access • Audit user access • Set up single sign-on to streamline access
Alliance Lead (Head of AWS Partnership, Director of Cloud Alliances)	Owns the AWS relationship and is responsible for driving growth of the AWS partnership through program alignment, co-sell readiness and cross-functional execution	• `AWSPartnerCentralFullAccess` • `AWSMarketplaceFullAccess` These policies combined provision these users with full read and write access to all features in AWS Partner Central. For a detailed breakdown of what this policy contains, see here.	• Manages ACE co-sell pipeline • Submits and tracks program applications • Oversees partner progress via the Scorecard and benefits eligibility • Approves MP listings, funding and program applications, solutions and marketing assets • Manages company profile • Defines user permissions requires and collaborates

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
			with IAM Administrator to provision access in IAM
Program Coordinator (Partner Operations Manager, Alliance Team Member, APN Program Administrator)	Collaborates closely with Alliance Lead to distribute oversight responsibilities by supporting tracking of requirements, management of submissions and ensuring compliance.	• `AWSPartnerCentralFullAccess` • `AWSMarketplaceFullAccess` These users are essentially an extension of the Alliance Lead and require similar permissions. These policies combined provisions these users with full read and write access to all features in AWS Partner Central. For a detailed breakdown of what this policy contains, see here.	• Tracks certifications, scorecard metrics and program deadlines • Submits documentation for programs, listings, solutions and funding • Coordinates across teams to gather and submit inputs • Handles operational issues

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
Marketing Manager (Partner Marketing Manager, Channel Marketing Lead)	The Marketing Manager builds awareness and drives demand for AWS-aligned offerings. They develop campaigns, create content, and apply for joint marketing programs.	• `AWSPartnerCentralMarketingManager` • `PartnerCentralIncentiveBenefitManagement` (only applicable if this persona is also responsible for managing funding programs/allocation)	• Create and list solutions and products on the AWS Marketplace • Create case studies • Manage campaigns • Manage funding such as Market Development Funds (MDF)

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
Sales Manager (Account Manager, Account Executive, Business Development Manager)	Accelerate revenue by sourcing, registering and closing AWS-related deals in collaboration with AWS field teams.	`AWSPartnerCentralOpportunityManagement` This policy grants users the ability to view and edit the entire pipeline of opportunities within your AWS Partner Central account. This policy is designed for team members who are actively working on partner opportunities and need access to opportunity management features, but don't require access to all Partner Central capabilities. This policy also provides access to other general purpose features, like the ability to access partner documentation, contact support, and track progress with the Scorecard.	• Registers co-sell opportunities • Accepts and manages AWS-referred leads • Maintains co-sell opportunity hygiene • Views pipeline metrics and reports on opportunity status and progress

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
Integration Engineer/ Developer	Technical user supporting the partner alliances team with building and maintaining CRM integrations connecting partner systems to AWS Partner Central APIs	`AWSFullAccessSandboxFullAccess`	• Design and implement integrations
Technical Lead	The Technical Lead is the engineer or architect who ensures their organization's solutions meet AWS technical standards and program requirements. They design and implement scalable cloud architectures, provide technical guidance across teams, and optimize solutions for performance, security, and cost.	• `AWSPartnerCentralFullAccess` • `AWSMarketplaceSellerProduct`	• Create solutions and submit Foundational Technical Reviews • Apply for programs or specializations and support with technical supporting documentation • Access to AWS technical documentation and enablement not available publicly

User persona	Persona Description	Recommended Partner Central Managed policies	Partner Central responsibilities
Funding Program Manager	The Funding Program Manager owns financial operations tied to AWS—tracking revenue, reconciling payments, and managing funding audits and reporting.	`PartnerCentralIncentiveBenefitManagement` This policy provides access to manage incentive and benefit programs within AWS Partner Central.	• Create new fund requests • Manage claims processes • View and manage all historical fund requests

AWS ProServe Tools Access

For services partners supporting customer migrations and who want access to the AWS Assessment Tools (outside of AWS Partner Central), users must be assigned one of three managed policies to be provisioned access. These tools include:

- **Migration Portfolio Assessment (MPA)**: A tool that helps partners and customers evaluate, plan, and prioritize workloads for migration to AWS. MPA enables partners to build a business case for migration, analyze the current application portfolio, estimate costs, and identify the right migration strategy for each workload. It provides data-driven insights to accelerate migration planning and reduce risk.
- **Assessment Tools (A2T)**: A suite of customer-facing survey and assessment tools, including the Migration Readiness Assessment (MRA) — a structured evaluation that measures a customer's readiness to migrate to AWS across six dimensions of the AWS Cloud Adoption Framework. A2T assessments help partners identify gaps, build remediation plans, and demonstrate migration readiness to AWS and the customer.

Access is controlled through three AWS managed policies, each mapped to a specific user persona. Use the table below to determine the level of access each individual requires:

User persona	Persona Description	Recommended Partner Central Managed policies	AWS Assessment Tools functionality
Individual Contributor	This individual creates and manages their own assessments in A2T and MPA. This is the base-level role required for all assessment activity.	`AWSPartnerProServeToolsIndividualContributor`	• Create, read, update, and share only their own assessments/portfolios in both A2T and MPA
Organization Reader and Individual Contributor	This individual requires visibility into all assessments across the organization, while also managing their own. This persona is common for team leads or senior practitioners who need to review historical or peer assessments without editing them.	`AWSPartnerProServeToolsOrganizationReaderIndividualContributor`	• Read all organizational assessments in A2T (read-only for others' work) • Create, read, update, and share only their own assessments/portfolios in both A2T and MPA
Organization Contributor (Full Assessment Access)	This individual requires full read/write access to all assessments in the organization. This persona is suited for senior practitioners or delivery leads who need to edit, delete, or share assessments	`AWSPartnerProServeToolsFullAccess`	• Create, edit, delete, and share any A2T assessments/MPA portfolios in the organization • Access to all historical A2T assessments/MPA portfolios created prior to partner migration to AWS Console

User persona	Persona Description	Recommended Partner Central Managed policies	AWS Assessment Tools functionality
	created by any user in the organization, including historical assessments.		

For more information about IAM managed policies, see Managing IAM policies. For information about attaching policies to users and groups, see Attaching a policy to an IAM user group.

User Management FAQs

Who in my organization is the IAM Administrator, and how do I contact them?

IAM Administrators typically sit within IT Security or Information Security departments, and sometimes in dedicated IAM teams or Governance/Compliance orgs. These Admins are generally responsible for implementing IAM policies, configuring SSO solutions, handling compliance reviews, and maintaining role-based access control structures.

What are the managed policy options for Partner Central in the AWS Consoles?

Refer to AWS managed policies for AWS Partner Central users for the most up-to-date documentation.

If I am unable to log in to my Partner Central account in the AWS Console, who do I contact?

Whether your organization uses an IdP, AWS IAM Identity Center without an IdP, or AWS Identity and Access Management console to manage AWS Partner Central access, your IAM Admin or IT department can help you with restoring access. AWS does not manage AWS account permissions.

Accessing AWS Partner Central

Users can sign in to AWS Partner Central from a browser. For the best experience, we recommend using a desktop computer.

To sign in to AWS Partner Central

1. Log into the AWS Management Console for the AWS account associated with their AWS Partner Central account.

   Depending on how users are managed in the account, this process will vary. Users using AWS IAM Identity Center will log in using Single Sign-On. Users with an external Identity Provider may log in through the IdP console and select the AWS account to log in.
2. Once logged into the AWS Management Console, users can get to the AWS Partner Central service page through:

   - Direct link)
   - Services menu
   - Global search
3. Choose **Launch AWS AWS Partner Central** on the service page.

Navigating AWS Partner Central

The AWS Partner Central dashboard features a navigation bar on the left side of the screen. This menu serves as your primary control center, providing quick access to key partner resources including AWS Partner benefits, training materials, and business growth tools. Additionally, partners who sell on the AWS Marketplace can use this navigation bar to manage their product listings and monitor sales performance.

Important

If you encounter an access error, it means your assigned IAM role lacks the necessary permissions. Check the error message for specific details and resolution steps. Review the AWS managed policies for AWS Partner Central users section for more information.

Note

While most Partner Central features are now in the AWS Console, some tools still use the legacy system. Users with appropriate IAM permissions are still able access those non-migrated features without additional login. Users will be prompted with a modal alerting them about the re-direction. When prompted, choose Sign In, which will automatically single sign-on users back to the legacy environment. Features that require this redirect include:

- Partner Scorecard
- Guides
- Program Applications
- Channel management tools

Similarly, all current AWS Marketplace Management Portal (AMMP) features will redirect users back to the legacy AMMP experience, without additional login. A new tab will open and the navigation bar will persist to enable users to seamlessly navigate between the different environments.

Navigation bar

All AWS Partner Central and AWS Marketplace Management Portal (AMMP) features are accessible from the unified navigation bar. Features are organized into AWS Partner Network (APN) journey phases: Build, Market, Sell and Grow. The below describes where each menu item and corresponding feature:

- **Partner scorecard:** View your Partner Scorecard to track progression in your AWS Partner path and tier requirements.
- **News and events:** The AWS Partner Central home page features Partner news and Partner events feeds. These feeds display curated collections of AWS and AWS Partner news and events relevant to AWS Partners.
- **Guides:** Access guides and documentation on topics around partner programs, AWS Services and more.

Build

- **Solutions:** Native in the AWS Console. Create and manage solutions. More information in the AWS Partner Central Builder Guide.
- **AI agents & tools:** Redirects to AMMP. Manage your AI agents and tools listings on the AWS Marketplace. For more information, see AI agent products.
- **SaaS products:** Redirects to AMMP. Manage your SaaS product listings on the AWS Marketplace. For more information, see SaaS-based products in AWS Marketplace.
- **Server products:** Redirects to AMMP. Manage your server product listings on the AWS Marketplace.
- **Machine learning products:** Redirects to AMMP. Manage machine learning (NL) algorithms and models that buyers can deploy in AWS. For more information, see Machine learning products in AWS Marketplace.
- **Amazon Machine Image:** Redirects to AMMP. Deliver products to buyers with Amazon Machine Images (AMIs). For more information, see AMI-based products in AWS Marketplace.
- **Data products:** Redirects to AMMP. Manage your data product listings on the AWS Marketplace. For more information, see Data products.
- **Professional services:** Redirects to AMMP. Manage your professional services listings on the AWS Marketplace. For more information, see Professional services products in AWS Marketplace.

- **Requests:** Redirects to AMMP. Displays a list of change requests made on products (AMI, Container, SaaS and Professional Services), offers, and other AWS Marketplace entities from AWS Marketplace Management Portal, or from AWS Marketplace Catalog API.
- **File upload:** Redirects to AMMP. Upload product load forms (PLFs) to request a new product or updates to an existing product in AWS Marketplace.
- **Device listings:** Redirects to the legacy Partner Central experience. Relevant for partners on the Hardware Path.

Go to Market

- **Marketing Central:** Redirects to AWS Marketing Central. Manage joint marketing campaign assets and resources.
- **Case studies:** Redirects to legacy Partner Central experience. Create and manage case studies to showcase customer wins.
- **Badge manager:** Redirects to the legacy Partner Central experience. Access and download AWS badges earned.

Sell

- **Leads:** Native in the AWS Console. Receive leads shared from AWS and convert them to co-sell opportunities.
- **Opportunities:** Native in the AWS Console. Accept and share opportunity invitations from AWS or other AWS Partners. Actively manage sales opportunities through the sales pipeline.
- **Private offers:** Redirects to AMMP. Create private offers for specific buyers, group multiple offers into private offer sets.
- **Public free trials:** Redirects to AMMP. Create public offers available to all buyers on AWS Marketplace.
- **Agreements:** Redirects to AMMP. Create public offers available to all buyers on AWS Marketplace.
- **Selling authorizations:** Redirects to AMMP.

Funding Benefits

For more information, see Managing fund requests in the AWS Partner Funding Portal.

- **Funding dashboard:** Native in the AWS Console. A centralized dashboard that provides real-time visibility into fund allocation, utilization, and performance metrics across various funding programs and initiatives.
- **Wallets:** Native in the AWS Console.

Channel management

For more information, see Channel Management.

- **Channel partner management:** Native in the AWS Console. Designed for partners who resell AWS services as an authorized AWS Channel Partner.
- **Distribution engagement requests:** Redirects to the legacy Partner Central. The Distributor engagement request is available for you to manage your new and existing requests to engage with an AWS Distributor.

Account connections

For more information, see Partner Connections.

- **Partner discovery:** Native in the AWS Console. Search and discover other AWS Partners to collaborate with.
- **Partner connections:** Native in the AWS Console. Connect with other AWS Partners to share and jointly manage customer opportunities.

Partner analytics

For more information, see Tracking progress with Partner analytics and Marketplace insights.

- **At a Glance:** Key metrics and account status.
- **Opportunities:** Analysis of your opportunity pipeline, with insights on estimated revenue, conversion success rates, etc.
- **Leads:** Monitor leads with conversion rate trends.
- **Investments:** Insights like claim rates and top funding sources on the Cash, Credits, and Discounts approved for your organization (if applicable).

- **Channel:** Summary of incentives earned from participating in the AWS Solution Provider and Distribution programs (if applicable), along with (if applicable) CEI Grow benefits, Partner Originated Discounts, Public Sector Discounts, and Partner Growth Discounts (formerly Partner Growth Rebate Credits).
- **Marketing Campaigns:** AWS-led marketing campaign summaries, with associated Lead and Opportunity metrics.
- **Training and Certifications:** View your teams' Training and Certification achievements, including certifications, accreditations, and trainings completed.

Marketplace insights

- **Agreements and renewals:** Native in the AWS Console. Provides information about agreements and renewals within 24 hours of signing an agreement in AWS Marketplace.
- **Usage:** Native in the AWS Console. Provides visualizations and fine-grained data for customers using SaaS and server usage-based products.
- **Billed revenue:** Native in the AWS Console. Provides information about billed revenue for accounting and other financial reporting purposes.
- **Collections and disbursements:** Native in the AWS Console. Provides information about funds that AWS collected and disbursed to your bank accounts since the previous disbursement.
- **Tax:** Native in the AWS Console. Provides information about taxes for seller transactions.

Partner admin

- **Program applications:** Redirects to legacy Partner Central experience. Apply for APN programs or manage active program applications.
- **Business plan:** Redirects to legacy Partner Central experience. Create and share joint business plans with AWS.
- **Profiles:** Native in the AWS Console. Create and manage your Partner and Seller profiles. For more information, see Creating and updating your profiles.
- **User onboarding:** Redirects to AWS IAM service in the AWS Console. For more information, see Onboarding users to your AWS Partner Central account.
- **Partner Central settings:** Native in the AWS Console. Manage your primary contact details, associated domains, and tags. For more information, see Managing settings in AWS Partner Central.

- **Marketplace settings:** Redirects to AMMP. Manage your AWS Marketplace settings including tax information. For more information, see Managing settings in AWS Partner Central.
- **Partner Central support:** Redirects to legacy Partner Central experience. Get help from the APN support team on APN-related queries.
- **Marketplace support:** Redirects to AMMP. Get help from the Marketplace support team on Marketplace listings and other Marketplace-related queries.
- **Marketplace refund support:** Redirects to AMMP. Request support for refunds on AWS Marketplace.

AWS Partner Central dashboard

The AWS Partner Central console dashboard provides a customizable interface that helps you track and manage your partnership with AWS. The dashboard features key widgets that display important information and guide you through essential actions.

Widgets

The Get Started widget is a prioritized list of recommended actions designed to help partners successfully co-sell with AWS and sell through AWS Marketplace. This widget displays tasks that partners should prioritize completing, and information they should maintain updated to provide AWS the information they need to provide personalized recommendations and allow you to unlock benefits.

Widgets can be reset, added, removed, or resized to customize the dashboard page to a specific user's preferences.

Search

The search box in the navigation bar provides a unified search tool for finding AWS services and features, service documentation, AWS Marketplace products, and more. AWS Partner Central users have access to partner-specific documentation and resources through the AWS Partner Assistant extension in Amazon Q, a benefit not available to standard AWS Console users. While general AWS Console search capabilities are accessible to all users, they do not include AWS Partner Network or AWS Partner Central specific documentation. To access partner-focused content, users can type AWS Partner Central related questions in the search bar and click **Ask Amazon Q** to launch the AWS Partner Assistant extension.

Languages

You can choose to customize the user interface to a different language. Select from 11 languages.

1. Click the Settings (##) icon in the upper right corner
2. Select your preferred language from the dropdown menu
3. The interface elements like buttons and labels will update to your chosen language

> **Note**
>
> While the interface will change, some content remains in English only, including legacy AWS Partner Central features such as News and Events, Partner Scorecard, and Guides.

Partner news and events

The AWS Partner Central home page features Partner news and Partner events feeds. These feeds display curated collections of AWS and AWS Partner news and events relevant to AWS Partners.

The Partner news feed features articles related to AWS Partner Central launch announcements, AWS service launch news, and important AWS Partner deadlines. To access a searchable and filterable list of articles published in the last six months, choose **View all partner news**.

The Partner events feed features events relevant to AWS Partners, including webinars, workshops, summits, and keynote events. Delivery-format tags indicate if an event is in-person, virtual, or both. Choose the title of an event to access more information or register. To access a searchable and filterable page of all upcoming events curated for AWS Partners, choose **View all partner events**. Pinned events display at the top of this page, highlighted because of their importance to all AWS Partners.

Personalized support from the AWS Partner Assistant extension in Amazon Q

Amazon Q (Q) is an AI-powered chat assistant available to all AWS customers in the AWS Management Console. When accessed from AWS Partner Central, Q will connect to Partner Assistant, an exclusive extension for AWS Partners that provides access to partner-specific content, including AWS Partner program documentation and guides not available to general AWS customers.

Personalization capabilities

Partner Assistant extension in Amazon Q also supports personalization capabilities. Users can receive guidance based on your specific partner profile, including your current Tier, Path or other account activity such as opportunities, solutions, benefits and AWS Marketplace listings.

> **Important**
>
> Use Amazon Q in AWS Partner Central to quickly find partner-specific information using natural language queries. Unlike the AWS Console's unified search tool, Amazon Q can provide summary based on partner-exclusive documentation to deliver answers and recommendations from Partner Central and Marketplace resources. Users can read source documentation by choosing the Source link below each chat response.

Language support

Partners can ask questions in non-English languages and receive responses in the same language. Supported non-English languages include:

- Mandarin
- French
- German
- Italian
- Japanese
- Spanish

- Korean
- Hindi
- Portuguese

Accessing Amazon Q for AWS Partner Central

1. From any page in the AWS Console, locate the Amazon Q logo from the top navigation
2. Click the Amazon Q logo to open the chat window

or

1. Type your question in natural language in search bar at the top of the AWS Management Console
2. Click Ask Amazon Q to open the chat window with your question filled in

Managing your account settings

From the navigation menu, partners have two settings: one for managing their AWS Partner Central account, and one for managing their Marketplace settings.

Topics

AWS Partner Central settings

In addition to capturing company profile details in the Partner and Seller profile sections, partners can manage other details, such as contact information, tags, and domains in the AWS Partner Central settings tab.

Navigate to the AWS Partner Central settings page from the left-hand navigation menu. At the top of the page, you will see a snapshot of your Account Summary, including:

- **Legal business name:** This Legal business name was provided during the Registration process. This name is only visible to you. To change how your company name appears to other AWS Partners or customers browsing the AWS Marketplace, navigate to Partner profiles menu item and update your Partner and/or Seller profile Display Name.
- **Partner Account status:** During Registration, if all account details were successfully verified, this will show as Active.
- **AWS Marketplace account status:** During Registration, an AWS Marketplace account was also created.

> **Note**
>
> The existence of an AWS Marketplace account does not mean all partners must sell on the AWS Marketplace. To list and sell your products or services on the AWS Marketplace, review the AWS Marketplace Seller Guide.

Beneath the Account Summary tab, you can manage specific AWS Partner Central account settings by selecting the corresponding tab.

Alliance lead contact

During Registration, contact details were collected, called the "alliance lead contact". This is the primary contact for the account. Only one contact can be added to an account. Additional contacts can be added to specific AWS resources, for example on a specific Opportunity, Fund Request or Support ticket. Contacts captured at the resource level will receive targeted communications related to that specific resource.

> **Important**
>
> All AWS Partner Network communications and key updates, such as the APN Newsletter or email announcements about changes in policies or new feature launches, will only be sent to this primary contact. For organizations who wish to distribute communications to a wider audience, we recommend using a shared email alias as the primary contact, which will allow for communication to go to all individuals with access to that shared inbox.

Additional contacts can be added within specific workflows, such as during opportunity and fund request creation, or program application submission. Specific notifications about these workflows, such as when an opportunity stage changes or when a fund request or program application is approved, will be sent to the individual contact collected within that workflow at the time of resource creation. These individual contact details can be updated within the resource itself.

Registered catalogs

When you create your product and the first version of your software, it's initially published in a limited scope so that only your account can access it. When you're ready, you can publish it to the AWS Marketplace catalog to allow buyers to subscribe and purchase your product.

Training and Certifications

Partners can manage the domains associated with their account for the purpose of Training and Certification access and credit in the Training and Certification tab.

Associating domains for AWS Training and Certification tracking

AWS uses Training and Certification achievements to validate technical expertise. These achievements are required for Tier progression and certain APN program eligibility.

Learners will log into Skill Builder by using their company email address and the "AWS Builder ID" login method. Based on the domains associated to their company's AWS Partner Central account, Skill Builder learners are granted access to partner-specific training content and the ability to manage the association of a personal certification email address within their Skill Builder profile.

> **Important**
>
> This represents a change in how learners access Skill Builder and associate certifications on personal email address with their company. For more information, review the Training and Certification Guide.

Partners can manage the domains associated to their account for the purpose of Training and Certification credit in the Training and Certification tab within AWS Partner Central settings.

Adding a domain

Associated domains are validated by a one-time-passcode sent to an email address that contains the desired domain. Ensure you have access to the email inbox that will receive the verification code to successfully complete the validation process.

> **Note**
>
> Only users with specific permissions assigned in IAM can add or remove domains. For more information on managing IAM permissions, see AWS managed policies for AWS Partner Central users.

1. Choose the **Associate domain** button
2. Enter in an e-mail address of the owned domain and choose **Send verification code**. Check for typos before sending.

> **Note**
>
> A code should be delivered to the entered email address in less than 5 minutes. If you did not receive the code, you have up to 5 attempts to receive the code. Once the code has been sent, you have 48 hours to enter the code into the text box for verification. If you are unable to receive a code, please reach out to the AWS Partner Central Support team via the left-side navigation menu.

3. Enter the code and choose **Associate domain**. If successful, you will be re-directed to the previous page and the newly associated domain will appear in the list of associated domains.

Removing a domain

1. Select the domain you wish to remove and the **Remove domain** button will activate.
2. Choose **Remove domain** or to un-do, choose **Clear selection**.
3. To ensure partners do not accidentally remove domains, users will see a prompt to manually type "remove" into a text box to proceed with removing a domain. Type in "remove" and then choose **Remove domain**.

Tags

Tags allow partners to label specific resources (such as Opportunities or Fund Requests) and control access based on these tags. For example, partners can tag opportunities by Region or Sector and restrict individual user access in IAM to these specific segments of their AWS Partner Central data.

Each tag has a key and a value. For each resource, each tag key must be unique and can only have one value. Don't include sensitive information in tags.

Create or update tags

Choose the Tags tab for a summary of all existing tags. To create a new tag:

1. Choose the **Create AWS Partner Central tag** button in the top right-hand corner.
2. From the Manage Partner Tags page, you can remove existing tags by choosing **Remove** next to the associated tag or choose **Add new tag** to create new ones.

Marketplace settings

For details on managing your Marketplace seller account, see here.

Creating solutions in AWS Partner Central

A solution is any product, service, or practice you offer to solve a customer business need. When you create a solution on AWS Partner Central, you provide details that help us understand what you bring to market. Eligible partners with validated solutions will be displayed on the Partner Solution Finder for customer discovery. Products can be attached to solutions to be listed and transacted on the AWS Marketplace. For more information about creating solutions, review the AWS Partner Central Builder Guide.

Co-selling with AWS

Partners participating in the APN Customer Engagements Program (ACE) can create, share and receive opportunities for collaboration with AWS. For more information on how to manage shared customer engagements with AWS, see the AWS Partner Central Sales Guide.

Tracking Partner Path and Tier Progression with the Partner Scorecard

AWS Partner Paths provide a tailored progression based on how a partner goes to market to AWS Customers. Enrolling in paths enables visibility into the AWS Partner Programs and benefits available based on your path(s) as you progress through the APN. Path selection is the first step in telling us what you do so we can provide your path to validation and specialization.

> **Important**
>
> If you need to remove a Partner Path from your account, you must contact APN Support for assistance.

Partner Scorecard – The Partner Scorecard is your tool to track progression of your AWS Partner path and tier requirements. The scorecard provides visibility into your achievements and requirements across your enrolled Partner Paths, helping you track your journey from enrolled to differentiated status.

Applying to AWS Partner programs

Programs provide resources through Partner Central, including technical training, marketing funds, and solution architect support to help partners grow their AWS-based business. Partners can apply to AWS Partner Programs in AWS Partner Central.

> **Note**
>
> Only users with specific managed policies assigned can apply for AWS Partner Programs. For more information, see AWS managed policies for AWS Partner Central users.

To apply for an AWS Partner program

1. Navigate to Partner Admin, Program Applications.
2. On the Applications and Programs page, choose **Create**.
3. On the Apply for Program page, choose **Select Designation**.
4. In the Select Designation dialog box, search for and choose a program.
5. Choose **Select**.
6. Select the acknowledgement checkbox and choose **Yes, I Agree**.
7. Complete the application steps. For more information, refer to the program guidelines.
8. To send your application, choose **Submit**. To save your application as a draft, choose **Submit Later**.

Managing fund requests in AWS Partner Central

AWS Partner Funding benefits are tailored to meet your business needs around training, new product and solution development, and go-to-market activities, enabling you to reach new customers and differentiate your business. AWS Partners may receive funding in the form of cash or AWS Promotional Credits depending on the specific funding option. Discover how to make the most of your available funding options and how to submit funding requests below.

AWS Partner Funding Benefits

This section shows all the Funding Programs that the Partner user has access to. If the blue **Create fund request** button is grayed out, the system has determined that the Partner account is not currently eligible for this type of funding due to Partner Path status or the lack of an MDF Wallet. Please review the eligibility for each program.

Accessing funding

To create, view, edit or manage fund requests, a user must be assigned the appropriate permissions in AWS IAM. For more information, see AWS managed policies for AWS Partner Central users. Please note that while a user may have access to the AWS Partner Funding Portal, they may not have anything to review or act on until their first Fund Request.

If a user is unable to access funding tools, please reach out to your IAM Administrator. You can also submit a Support Case via AWS Partner Central in the AWS Console for General APN Support.

To access funding tools:

1. Log into AWS Partner Central in the AWS Console
2. Click on **Launch AWS Partner Central** in the middle of the home screen.
3. Select **Funding dashboard** under **Funding Benefits** on the lefthand navigation pane
4. Users can begin submitting Fund Requests from this page in Partner Central
    a. Click the **Create fund request** button and a dropdown selection of eligible programs will appear
    b. The subsequent templates will route the user to create a Fund Request for the core programs offered

5. Users can also navigate to the **AWS Partner Funding Benefits** tab to review eligible core programs

Managing fund requests

The Partner Funding Dashboard is the main place to review all of your Fund Requests and claims regardless of stage and/or status, in one place for all supported programs. There are two main sections, Funding Activities and AWS Partner Funding Benefits.

On the Partner Funding Dashboard landing page, users with the appropriate permissions will see a summary of all Fund Requests, regardless of status or stage.

Funding Activities

This section shows all the Fund Requests (all statuses and stages) that the Partner user has access to. For standard APUs, they can see the requests they are the owner of, including drafted. ALs can see all requests for the Partner account regardless of owner.

There are multiple ways to find a fund request:

- **Fund request ID** — filter for the specific ID of the fund request
- **Fund request stage** — filter by what approval stage the request is in (AWS Review, Business Approval, Finance Approval, etc.)
- **Fund request status** — filter by the status the request is in (active, cancelled, completed, etc.)
- **Funding type** — filter by the type of funding (cash or credit)
- **Program** — filter by the overall template used for each request (MDF, MAP, PIF, Misc., etc.)
- **Subcategory** — filter by the program each request is under (MDF, MAP, Sandbox, WMP, SCA, etc.)
- **Purchase order number** — filter for the specific purchase order number
- **Opportunity ID** — filter for the specific opportunity ID
- **Budget Year** — filter by the budget year the request is tied to

There are 4 possible actions to take in this dashboard:

- **Export** — Exports the displayed list of Funding Activities to an Excel Spreadsheet
- **Create Fund Request** — Allows a Partner to submit a Fund Request with a dropdown by program
- **Cancel Fund Request** — Allows a Partner to Delete a Fund Request from their dashboard

- **View Details** — Allows a partner to view specific details of a selected fund request

Creating a fund request

Users can create a new Fund Request from the Funding Dashboard page. To create a new Fund Request:

1. Choose **Create Fund Request**
2. A dropdown list will appear with a list of funding programs.
3. Choose the relevant funding program by selecting the name in the picklist

Once a Fund Request has been submitted, it goes through a series of review and validation processes, depending on specific program requirements. Partners can track the progress of a Fund Request as it goes through these approval workflows based on two attributes: the Stage and the Status. The Fund Request Stage indicates the current phase in the overall Fund Request lifecycle, while the Status indicates the current health or condition of the Fund Request (i.e. Pending, In Review, Approved).

Fund request stages

The table below details the stages that a Fund Request can be in as it goes through the approval lifecycle. See more details for who the assigned Approver is for each stage is by program in the Approval Workflow section of the guide.

Stage	Description
Created	The request is still in draft and has not been submitted by the Partner to AWS, OR The request has been rejected and is now pending Partner updates and resubmission.
AWS Review	The request is with the AWS Reviewer in AWS. This stage is only applicable for Sell (POC) and Miscellaneous (Jumpstart and ISV WMP) funding motions.
Tech Approval	This stage indicates that the Fund Request is with the Partner Solution Architect to ensure technical feasibility of the project plan/statement

Stage	Description
	of work. This stage is only applicable for Sell Motion Funding programs (POC).
Business Approval	The Fund Request is pending review and approval by the assigned Business Approver. The Business Approver varies by program.
Finance Approval	The Fund Request is with the AWS Operations team to generate a Purchase Order (PO) for Cash requests, AND/OR generating codes for Credit requests.
Pre-Approval	This stage indicates that the Fund Request has obtained all necessary approvals and the Partner can begin executing their activity/project. For credit, the request will remain in this stage until all credit codes have been disbursed and applied. For requests including cash, this is pending final finance confirmation before moving to Cash Claim stage. For MAP requests, this pass-through stage does not exist, the Fund Request being in Cash Claim stage indicates pre-approval.
Cash Claim	The Partner is able to submit a Cash Claim when the project (or milestone) is complete. The Partner submits the actuals for the claim(s), and AWS reviews and rejects/approves the actuals in this stage. Migrated Partners will see “Awaiting Approval” in the Cash Claim Status section under Cash claim plans once the claim actuals are submitted. Once the actuals are approved, the Fund Request will provide a link to Payee Central for the Partner to submit invoice. This stage will not update until the invoice is approved.
Completed	All credits have been redeemed for the relevant FR AND/OR all cash claims have been completed. No further action is required.

Fund request statuses

The table below details the statuses that a Fund Request can be in and indicates the current health of the Fund Request. The status will be found in the Project Details section of the Fund Request.

Status	Description
Active	This is the first status that a record will receive. It will stay in this status through most of its lifecycle.
Pending	For most Fund Requests, this status is temporary, the request is synching. Status will revert to Active status upon successful sync.
Terminated	The Partner has cancelled the request. Once a request has been terminated, it cannot be reactivated.
Expired	In the situation where a Fund Request has passed its expiration date (30 days after delivery end date), the system will update the status of the request to expired. Fund Request can no longer have actions taken.
Completed	Completed is the status once all invoice details have been added to the Fund Request by AWS, and/or credit codes have been redeemed and there is no further action required.
Deleted	Deleted is the status of a Fund Request if the Partner has deleted it from their dashboard view. This action can only be taken on Fund Requests in the Created stage (either never submitted, or rejected back to the Partner). Deleted fund requests will no longer show in the partner dashboard, and may no longer be viewed or retrieved

Attachment statuses

The table below details the statuses that an attachment can reflect. These statuses apply to both Fund Request Attachments and Claim Attachments.

Status	Description
PendingUpload	The document is currently being uploaded.
Scanning	The document has been attached and is currently being scanned for compliance with Application Security. This status does not prevent submission of the Fund Request or Claim

Status	Description
ScannedClean	The document has been attached, and scanning has been completed, no problems found
Quarantined	The file was scanned and does not meet criteria set by Application Security. Usually this means it contains a formula that is not among the accepted set of formulas allowed by the tool. The document should be updated to remove formulas and reattached or converted to a PDF and reattached.

Updating a fund request

Once a Fund Request has been submitted, users can edit or update details by recalling a Fund Request. The Recall function will bring the Fund Request back to the Created stage where users can perform edits. The Recall function is only available for Fund Requests prior to entering the Pre-Approval Stage, at which point, the Fund Request can no longer be recalled.

To Recall a Fund Request:

1. Select the Fund Request ID from the Funding Dashboard by choosing the relevant Fund Request
2. Choose the **Recall** button
3. Users will be returned to Step 1 of the Fund Request submission process, where all pre-existing information will be available.
4. Edit the details fields as needed
5. Resubmit the fund request by choosing **Submit**

Cancelling a fund request

The Cancel function can be used when a Partner needs to cancel a Fund Request that will no longer be executed. Once the Fund Request has been canceled, the status will change from "Active" to "Cancel" but the stage will not change. The Fund Request will also continue to be visible in the funding dashboard. By canceling, the Partner will no longer be able to edit, submit, resubmit, or view the Fund Request. The Cancel function can be performed at any time prior to entering the Completed Stage, at which point, the Fund Request can no longer be canceled.

To cancel a Fund Request:

1. Select the Fund Request ID from the funding dashboard
2. Choose **Cancel fund request** from the Fund Request summary screen.

Resubmitting a fund request or claim

If a Fund Request or Claim has been rejected, it can be revised and resubmitted.

> **Important**
>
> The rejection reason is not visible from this workflow, so review the rejection reason first.

To resubmit a fund request:

1. Open the Fund Request from the dashboard by selecting the hyperlink of the Fund Request ID
2. The rejection reason will be in the automatic rejection email, and can also be seen in the Fund Request by choosing **Approval History** in the action bar, or scrolling down to the bottom section of the Fund Request.
3. Review the rejection reason first, then choose **Resume fund request** from the action bar at the top of the request.
4. Resume fund request opens the Fund Request for revision and resubmission. It will reopen the initial submission workflow for the program and allow the Partner to edit the details, and at the end, officially resubmit. The rejection reason is not visible from this workflow, so review the rejection reason first. The start date will need to be moved out 14 days from the current date, if the previous date is not already enough in the future.
5. If an error is encountered, choose **Fix** to see what fields need to be corrected.
6. Once all information is updated, choose **Submit fund request** to resubmit the Fund Request.

To resubmit a claim:

1. Open the Fund Request from the dashboard by selecting the hyperlink of the Fund Request ID.
2. The rejection reason will be in the automatic rejection email and can also be seen in the Fund Request under the "Actuals" section on the Cash Claim page.

3. Review the rejection reason first, then make any necessary updates to the Claim Actuals and select **Edit cash claim** from the Cash claim plans section of the request.
4. The **Edit cash claim** button opens the Claim for revision and resubmission. It will reopen the claim submission workflow and allow the Partner to edit the details, and at the end, officially resubmit. The rejection reason is not visible from this workflow, so review the rejection reason first.
5. Once all necessary updates are made, select **Submit cash claim actual** to resubmit the claim.

Extending a fund request

The Extend function can be used when a Partner needs to modify the planned delivery end date of an approved Fund Request. AWS Partners can self-extend the planned delivery end date of an approved activity in the AWS Partner Funding Portal one time up to 90 days based on standard Funding Program policy. Once the dates are extended, the Funding Expiration Date will automatically update accordingly.

Extension guidelines

Before an activity expires, the Fund Request can be extended once up to 90 days.

Extended date requirements:

- Must be 1-90 days from the original planned delivery end date
- Cannot be between 12/16 and 1/1
- Cannot cross years for MDF

Important notes

- Once the activity completion date is extended, the Funding Expiration Date will automatically update to 30 days from the new completion date or December 15th of the calendar year of the request. If December 15th is selected as the end date, the expiration will be the same day.
- Claims must be submitted within 30 days after the activity completion date or by December 15th of the calendar year of the request.
- Invoices should be submitted in Payee Central after Claim approval, and prior to the Expiration Date.

To extend a fund request:

1. Select the Fund Request ID from the funding dashboard by choosing the relevant Fund Request
2. Choose the **Extend fund request** button on the upper right corner of the page
3. Enter the new project end date following the extension guidelines above
4. Extend the fund request by choosing **Extend fund request**

Using agents for funding recommendations and fund requests

AWS Partner Central agents analyze your opportunities against available funding programs and can create fund requests directly from the opportunity details page.

Prerequisites

- Your account has migrated to AWS Partner Central in the AWS Management Console.
- Your IAM user or role has the required permissions:
  - `partnercentral:ListBenefitAllocations`
  - `partnercentral:ListBenefitApplications`
  - `partnercentral:CreateBenefitApplication`
  - `partnercentral:GetBenefitApplication`
  - `partnercentral:UpdateBenefitApplication`
  - `partnercentral:AssociateBenefitApplicationResource`
  - `partnercentral:DisassociateBenefitApplicationResource`
  - `partnercentral:GetOpportunity`
  - `partnercentral:GetAwsOpporunitySummary`
  - `partnercentral:UseSession`
  - `aws-marketplace:DescribeEntity`
  - `aws-marketplace:SearchAgreements`
- You have at least one active opportunity.

How funding recommendations work

When you open an opportunity details page, the **Funding Recommendation** widget automatically evaluates the opportunity against available AWS funding programs based on opportunity stage, expected revenue, customer use case, and partner path eligibility.

If a match is found, the widget displays the following information:

Element	Description
Program name	The recommended funding program.
Program description	A summary from AWS funding documentation.
Reason for recommendation	Why this opportunity may qualify, based on stage, ARR, and use case.

> **Note**
>
> Funding recommendations are provided for informational purposes to help identify potentially relevant programs. Recommendations do not guarantee funding approval or eligibility.

The widget provides three actions:

Action	Description
Get estimated funding	Calculates potential funding based on opportunity value and program rules.
Create fund request	Starts a draft fund request auto-populated with opportunity data.
Learn about funding programs	Opens a conversational interface for funding questions.

If no match is found, the widget indicates this and offers a **Learn about funding programs** button.

When a recommended program is associated with a Standard Strategic Collaboration Agreement (SCA), the feature also displays SCA budget allocation information — what has been allocated and what remains available.

> **Note**
>
> The agent does not access the SCA agreement document itself. SCA agreements are managed in Contract Central.

Getting a funding recommendation

1. Navigate to **Opportunities** in the left navigation.
2. Select an opportunity.
3. Locate the **Funding Recommendation** widget on the opportunity details page.
4. Review the recommendation and choose an action.

You can also choose **Ask about this opportunity** and ask questions such as "What funding programs are available?" or "Why was this program recommended?"

Creating a fund request

1. In the **Funding Recommendation** widget, choose **Create fund request**.
2. The agent collects data from the opportunity record.
3. If information is missing, the agent asks clarifying questions in the chat interface.
4. The agent generates a draft and provides a link.
5. Open the link to review the draft in the AWS Funding portal, then submit.

After submission, the request follows the standard approval workflow. Track progress on the **Funding Dashboard**. For more information, see the section called “Creating a fund request”.

You can also start this process through the chat interface by choosing **Ask about this opportunity** and typing "Create a fund request for this opportunity."

Important considerations

Consideration	Details
Eligibility	Recommendations are based on available data. Final eligibility is determined during the application review.
Data scope	The agent uses only your opportunity and partner account data.
Permissions	Users without fund request permissions receive an access denied message.
Sessions	Conversations are session-based, not persisted. Each interaction has a unique Session ID.

Related resources

- *Managing fund requests in AWS Partner Central*
- the section called “Creating a fund request”
- AWS Partner Funding Benefits

Connecting with other AWS partners

AWS Partner Central facilitates collaboration between AWS partners, allowing them to connect and share opportunities with each other. Partners can discover, connect and manage multi-partner engagements. For more information, review the Partner Connections section of the AWS Partner Central Sales Guide.

Channel Management

AWS Partner Central Channel Management provides AWS Solution Providers, Distributors, and Distribution Sellers (Channel Partners) with capabilities to manage their AWS accounts participating in Channel Programs. AWS Partner Central Channel Management is used with AWS Billing Transfer to enable channel partners to resell to end customers while customers retain root access to their own AWS management account.

Key capabilities include:

- Centrally manage AWS accounts used for reselling
- Establish, track, and manage relationships with customers and distribution sellers
- Qualify for partner program benefits and discounts
- Monitor billing transfer relationships across multiple accounts

Prerequisites:

- Active registration in AWS Channel Programs (Solution Provider, Distribution, or Distribution Seller)
- AWS Partner Central account with linked AWS account
- AWS Partner Central user with mapped Partner Central Channel IAM roles
- Necessary IAM roles provisioned in the AWS accounts used in channel management
- AWS Partner Central user with mapped Partner Central Channel IAM roles
- Active AWS management account used to receive bills and administer channel programs

> **Important**
>
> AWS Partner Central channel management features require IAM roles to be configured in both the Partner Central linked AWS account and the AWS management account used to receive bills and administer channel programs. Work with your AWS Partner Central cloud admin to ensure IAM permissions are configured, and work with your alliance lead or cloud admin to map IAM roles to Partner Central users. Learn more about accessing channel management in the API reference.

How AWS Partner Central channel management works

The Channel Management workflow follows a structured process to set up and manage your resale business. Here's how the components work together:

1. **Create and activate Program Management Accounts**

   Report your AWS management accounts as PMAs to associate them with your channel program authorization. Activate your program management accounts instantly using channel handshakes to verify consent from the AWS management account.

2. **Establish relationships with customers or distribution sellers**

   Create relationships to define how you work with each customer or downstream seller AWS management account and qualify for channel program benefits. Select appropriate support models and settings for each relationship.

3. **Set up service periods to manage billing transfer offboarding (optional)**

   Add service periods to relationships to enforce minimum notice periods or fixed commitment periods on billing transfer. Partner service periods are added to govern changes to billing transfer, and must be accepted by the customer's AWS management account.

4. **Monitor billing transfer status and relationship list**

   Track the status of billing transfers across all program management accounts and relationships from a central location.

Program management accounts

A program management account (PMA) is an AWS management account that you use to manage your AWS Channel Program participation and relationships with customer or distribution seller AWS accounts. Each PMA is associated with a single AWS Channel Program (AWS Solution Provider, AWS Distribution, or AWS Distribution Seller).

Topics

Creating a program management account

To create a program management account, you will need an AWS management account ID and an active channel program registration.

Member accounts and standalone accounts cannot be used as PMAs. Additionally, you can not use an AWS Management Account that is already onboarded as a payer account in legacy Partner Central Channel Management. You must first offboard the legacy payer account prior to creating a PMA with the same account ID.

Common scenarios for creating a new PMA include:

- Expanding into a new geographic region with different billing requirements
- Setting up a dedicated account for a specific business division
- Separating management of different AWS Channel Programs

To create a PMA

1. Navigate to Channel Management in AWS Partner Central.
2. On the program management accounts tab, choose **Create**.
3. Enter AWS management account ID.
4. Select Channel Program type.
5. (Optional) Add descriptive name for the PMA.
6. Submit for activation.

Activating a program management account

To activate a PMA, a channel handshake must be accepted by the AWS management account.

For AWS Partner Central UI users:

- The channel handshake is automatically created when you create a PMA
- The root email address of the AWS management account receives an request email
- An authorized user must access the invited AWS management account using the unique link provided in the request email

- Within the AWS console of the invited management account, they can accept or reject the request

For CLI/SDK users:

- You must explicitly send a program management account channel handshake request
- The root email address of the AWS management account receives an request email
- The account owner must either access the invited AWS management account and accept/reject through the AWS console using the provided unique link in the request email, or use CLI commands from the invited AWS management account to accept/reject the handshake

> **Important**
>
> The handshake request can only be accepted or rejected by signing in to or accessing the invited AWS management account. The partner who created the PMA in Partner Central must have access to this management account to complete the activation process.

Channel relationships

Channel relationships in AWS Partner Central provide a centralized way to manage connections between your program management accounts and your customer, distribution seller, or internal AWS Organizations.

Channel Management supports three types of relationships:

- **End Customer:** Direct resale relationships with organizations purchasing AWS services
- **Distribution Seller:** Downstream resale partners operating under your distribution agreement (for Distributors only)
- **Internal:** Partner's own AWS consumption related to testing and development of their channel business

Topics

Creating a relationship

When creating a new relationship, you'll need to provide specific information to properly configure the connection:

Required information:

- AWS management account ID of customer/seller organization
- Relationship type
- Customer sector (Government/Commercial)
- Account model (Solution Provider Terms Model [SPTM]/End Customer Account Model [ECAM])
- Support model

> **Note**
>
> The relationship reported must match your Channel Programs agreement. You can only select relationship details that align with the account models and sectors you are authorized to resell to.

Selecting a support model

Support relationships define how you'll provide support to your customers. You can apply unique support models to each relationship while serving customers and distribution sellers from a single PMA.

Support model options:

- **Keep existing support model:** Maintain current support plan
- **Resold support:** Replace the current support plan with a new plan at resold pricing
- **Partner-Led support:** If eligible, manage support for your customer directly

Support details:

- **TAM location preference:** Choose preferred region for AWS Technical Account Manager
- **Support coverage scope:** Define whether support applies to management account or entire organization

- **Charge account ID:** Specify billing account for consolidated support invoicing, if applicable
- **Support provider:** If you are a distribution seller electing PLS on an end customer account, designate who is providing support to the customer

Service periods

Service periods create mutual agreements that prevent unilateral changes to billing transfers during specified commitment periods. Partners can establish either minimum notice requirements or fixed-term commitments, providing flexibility to align with existing service contracts and business needs. Service periods are associated with channel relationships, and provide additional governance options to channel relationships.

Service periods support two types of agreements:

- **Minimum notice periods** – Require 14, 30, or 60 days advance notice before either party can modify or terminate the billing transfer relationship
- **Fixed-term commitments** – Establish binding agreements for up to 1 year that align with service contracts

Topics

Creating a service period

Service periods can be added to any channel relationship using Partner Central Channel Management.

1. **Initiate the service period** – Channel Partners create service period invitations on specific relationships, specifying either minimum notice requirements (14, 30, or 60 days) or fixed-term commitments (60-365 days).
2. **Customer notification** – A channel handshake is automatically created and the end-customer's AWS management account receives an email notification with a unique response link.

3. **Customer review and response** – An authorized user from the customer's AWS management account must:
    - Access the invitation using the unique link provided in the email
    - Sign in to their AWS Console to review the proposed service period terms
    - Accept or reject the service period agreement
4. **Service period activation** – Once the customer accepts the channel handshake, the service period becomes active and governs the billing transfer relationship according to the agreed terms.

Managing an active service period

Active service periods impact both parties Billing Transfer management experience in Billing and Cost Management console. Partners can view and manage active service periods through AWS Partner Central channel management.

- **Fixed-term commitments** prevent either party from modifying the billing transfer until the commitment period expires
- **Minimum notice periods** require the specified advance notice for any billing transfer changes

Replacing service periods

Partners may need to replace an existing active service period with new terms to accommodate changing business requirements or contract renewals. The replacement process ensures continuous governance of the billing transfer relationship while updating the service period parameters.

When to replace a service period

- Converting from a minimum notice period to a fixed-term commitment (or vice versa)
- Extending or modifying the duration of a fixed-term commitment
- Adjusting minimum notice period requirements (e.g., changing from 30 to 60 days)
- Renewing an expiring fixed-term commitment with updated terms

Replacement process

1. **Partner initiates replacement** – Channel Partners access the active service period through AWS Partner Central channel relationship management and select the option to replace the service period. Partners specify the new service period terms (either updated minimum notice days or new start/end dates for fixed-term commitments) and can include optional context explaining the reason for replacement.
2. **Customer notification** – A new service period channel handshake is automatically created and the end-customer's AWS management account receives an email notification with a unique link to review the proposed replacement terms.
3. **Customer review and response** – An authorized user from the customer's AWS management account must:
   - Access the replacement request using the provided link
   - Sign in to the AWS Console to review the new service period terms and partner's explanation
   - Accept or reject the replacement request
4. **Seamless transition** – When the customer accepts the replacement handshake:
   - The previous service period ends immediately
   - The new service period becomes active with the updated terms
   - The billing transfer relationship continues uninterrupted under the new service period governance
   - Both parties receive confirmation notifications

Important considerations

- If the customer rejects the replacement request, the original service period continues under its existing terms
- Only one pending service period handshake can exist at a time for each relationship
- Replacement requests expire after 30 days if not accepted by the customer
- The replacement history is maintained in the relationship record for audit purposes
- Replacing a service period does not affect the underlying billing transfer relationship

Early termination

Partners can request early termination of service periods before their natural expiration, but both parties must mutually consent through another channel handshake process.

Who can initiate termination:

- Only Channel Partners can initiate early termination requests
- End-customers cannot directly request termination through the AWS Console
- Customers who wish to end a service period early should contact their Channel Partner to request termination

Termination process:

1. **Partner initiates request** – Channel Partners access the active service period through AWS Partner Central and select the option to end the agreement early. Partners can include optional context explaining the reason for termination.
2. **Customer notification** – A termination channel handshake is created and the end-customer receives an email notification with a unique link to review the termination request.
3. **Customer review and consent** – An authorized user from the customer's AWS management account must:
   - Access the termination request using the provided link
   - Sign in to the AWS Console to review the termination details and partner's explanation
   - Accept or reject the early termination request
4. **Immediate effect** – When the customer accepts the termination handshake:
   - The service period ends immediately
   - Both parties instantly regain full control over the billing transfer relationship
   - Standard billing transfer management becomes available again through the AWS Billing and Cost Management console
   - Both parties receive confirmation notifications

Important considerations:

- If the customer rejects the termination request, the service period continues under its original terms
- Terminating a service period only ends the agreement – it does not automatically sever the underlying billing transfer
- After termination, either party can manage the billing transfer according to standard AWS procedures
- Terminated service periods remain visible in the relationship history for audit purposes

Migrating legacy channel accounts

This guide explains how AWS Channel Partners can migrate their existing channel end customers in partner-controlled AWS Organizations to billing transfer, enabling customers to maintain independent AWS Organizations while partners retain billing responsibility.

Channel Partners have two options to migrate existing end customer accounts to billing transfer:

Full Organization Transfer

Transfer your existing AWS Organization to customer ownership while maintaining billing responsibility through billing transfer. This process involves transferring root account ownership to the customer after establishing billing transfer, preserving all existing organization configurations and service integrations.

Benefits:

- Maintains all existing organization configurations
- Minimizes technical complexity and migration time
- Preserves service dependencies and integrations

Important Considerations:

- Best suited for single-tenant organizations
- Historical billing data becomes visible to the customer
- Partner must set up billing transfer before transferring root ownership

Member Account Transfer

Move individual member accounts from your existing AWS Organization to a new customer-owned Organization. This process involves creating a new Organization for the customer, establishing billing transfer, then migrating member accounts.

Benefits:

- Maintains billing privacy throughout migration
- Provides flexibility in migration scheduling
- Works for both single-tenant and multi-tenant organizations

Important Considerations:

- Requires rebuilding Organization-level configurations
- Organization-level dependencies must be identified and recreated
- Longer migration timeline than full organization transfer

Transferring Organization ownership

This migration path transfers root account ownership of an existing AWS Organization to your customer while maintaining billing responsibility through billing transfer.

Prerequisites:

- Organization must be in all-features mode
- Customer must have an email for root account ownership
- Organization serves one customer's workloads

Migration Steps:

To ensure continuous discount application throughout the migration process without any gaps, follow these steps:

1. **Define a new Partner Management Account (PMA)**

Create a new AWS account that will serve as your Partner Management Account and register this account as a PMA in Partner Central. This account will be responsible for the billing and payment for the customer organization.

2. **Identify the management account of the existing customer to migrate**

   Identify the AWS account currently serving as the management account (legacy payer account) of the customer's organization that you wish to migrate to billing transfer.

3. **Establish a Partner Central channel relationship**

   Create a channel relationship in Partner Central between your new Partner Management Account (from step 1) and the customer's legacy payer account (from step 2). As this organization contains your end customers workloads, you can add the account as an "end customer" relationship.

4. **Set up billing transfer**

   From your new Partner Management Account, navigate to the AWS Billing and Cost Management console. Select Billing Transfers and create a new transfer by entering your customer's AWS management account ID. Your customer will receive an email notification and must accept the transfer in their AWS console.

5. **Wait for Billing Transfer to become effective**

   Wait until the billing transfer becomes active, which occurs on the 1st day of the following month after acceptance. Do not proceed with the next steps until the billing transfer is active.

6. **Prepare the organization for transfer**

   Update the management account's billing information in the AWS Billing and Cost Management console to reflect your customer's details.

7. **Transfer root account ownership**

   Sign in to the Organization's root account and navigate to My Account in the AWS Management Console. Remove any partner MFA devices or other partner-specific security configurations. Update the root user email address to your customer's domain. The customer will receive an email to activate their root account access. Complete this step within 60 days of billing transfer going into effect.

8. **Verify transfer completion**

After the customer accepts ownership, verify that billing transfer remains active and your organization continues receiving invoices. The customer should now have full root access to manage their organization while billing responsibility remains with your organization through the established billing transfer.

> **Important**
>
> While full Organization transfer is the technically simplest path for migration, partners should be aware that this approach will expose their historical billing data to the new organization owner. This includes all billing information such as pricing, reserved instances, and saving plans that existed before the transfer of ownership.

Transferring member accounts

This migration path moves individual member accounts from your existing AWS Organization to a new customer-owned organization, while maintaining billing responsibility through billing transfer.

Prerequisites:

- Customer needs a management account for their new organization
- List of member accounts to be transferred
- Documentation of any organizational dependencies within each member account to be transferred

Migration Steps:

1. **Set up Customer's new Organization**

   First, establish the destination for member accounts. The customer must either create a new AWS account or designate an existing account to serve as their management account. In the AWS Organizations console of this account, enable AWS Organizations and configure initial organization settings. This creates the target environment for the member accounts.
2. **Establish billing transfer**

   Before moving any member accounts, set up billing transfer to ensure continuous billing responsibility. In AWS Partner Central, create a billing transfer from the customer's new

management account to your Program Management Account (PMA). The customer must accept this transfer in their AWS Billing and Cost Management console. Wait for the billing transfer to become active on the first of the next month before proceeding with account migration.

3. **Prepare member account migration**

   Review organization-level dependencies for the member accounts you plan to migrate. Remove or document any service control policies, resource sharing configurations, or delegated administrator settings that will need to be rebuilt in the new organization. Ensure you have a plan to reconstruct necessary configurations in the customer's organization.

4. **Transfer member accounts**

   Once billing transfer is active, begin the account migration process. From the customer's new Organization, send invitations to each member account you want to transfer. Sign in to each member account to accept these invitations. Member accounts will then leave the legacy partner Organization and join the customer's Organization. Coordinate with the end customer to rebuild any necessary organizational configurations in their new environment.

> ⚠ **Important**
>
> Ensure billing transfer is active before initiating any member account transfers. This maintains proper billing responsibility throughout the migration process.

Mapping IAM roles to a channel management user

This section explains how to map AWS Partner Central AWS Identity and Access Management (IAM) roles to your channel management service users on AWS Partner Central. This IAM role mapping is required to enable Partner Central users to access Partner Central Channel Management features. Mapping enables Partner Central Channel Management users to perform actions on the AWS Partner Central AWS account. Selecting an IAM role to access AWS Partner Central Channel APIs by Partner Central users enables features such as Channel Program Management Account and Relationship management.

Before mapping, you must first complete the following:

- Link your AWS Partner Central account to a Partner Central linked AWS account.

- Create IAM roles in the AWS Partner Central linked AWS account.
- While creating IAM roles, add the `AWSPartnerCentralChannelManagement` managed policy to the role to grant AWS Partner Central users permissions to perform channel management actions. For more information, refer to Managed policies for AWS Partner Central users.
- Add the following custom trust policy to the IAM roles, to allow AWS Partner Central to map the AWS IAM roles.

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

  "Statement": [
    {
            "Effect": "Allow",
            "Principal": {
                "Service": "partnercentral-account-management.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
  ]
}
```

To map an AWS Partner Central IAM role to a non-cloud admin user

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **AWS account linking** section of the AWS Partner Central homepage, choose **Manage Linked Account**.
3. On the **AWS account linking**, page, select **Manage IAM roles**.
4. In the non-cloud admin user section, select the partner users you wish to grant access, then choose **Map IAM role**.
5. Choose the IAM role created containing the above channel policy from the dropdown list.
6. Choose **Map role**.

To unmap an AWS Partner Central IAM role from a non-cloud admin user

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **AWS account linking** section of the AWS Partner Central homepage, choose **Manage Linked Account**.

3. On the **AWS account linking**, page, select **Manage IAM roles**.
4. In the non-cloud admin user section, select the partner users you wish to revoke access, then choose **Unmap IAM role**.
5. Choose the IAM role from the dropdown list.
6. Choose **Unmap role**.

> **Important**
>
> AWS Partner Central channel management features require IAM roles to be configured in both the Partner Central linked AWS account and the AWS management account used to receive bills and administer channel programs. Work with your AWS Partner Central cloud admin to ensure IAM permissions are configured, and work with your alliance lead or cloud admin to map IAM roles to Partner Central users. Learn more about accessing channel management in the API reference.

Tracking progress with Partner analytics and Marketplace insights

The Partner analytics and Marketplace insights dashboards provide AWS Partners and Marketplace Sellers with real-time insights into their product performance, including customer usage patterns, revenue trends, and subscription metrics through interactive visualizations and customizable reports. Marketplace Sellers can track key performance indicators like monthly recurring revenue, customer acquisition costs, conversion rates, and geographic distribution of customers, enabling data-driven decisions to optimize their AWS Marketplace strategy.

> **Note**
>
> Partner analytics pages without sufficient data will not work as expected. Users will see an error. To determine if the error is due to IAM permissions vs insufficient data, users can navigate to specific dashboards with different data sources.

For more information, see Navigating AWS Partner Central. You can reference the AWS managed policies for AWS Partner Central users documentation to review access policies for the dashboards.

Topics

Partner Analytics Dashboard

Partner Analytics includes 8 dashboards that let you filter, sort, and drill down on the data you need to manage your ACE Opportunities and Leads, Investments, AWS-led Marketing Campaigns, and Trainings and Certifications. To navigate across dashboards within the dashboard, simply click on the desired dashboard.

The 8 dashboards are:

- At a Glance: Comprehensive visualization of cross-functional KPIs and critical success metrics aggregated from core operational domains.

- Opportunities: Quantitative analysis of AWS and Partner-referred opportunity flows, featuring pipeline velocity metrics, revenue forecasting models, and statistical conversion analytics.
- Leads: Systematic tracking of lead acquisition and progression, with granular conversion rate analysis and source attribution metrics.
- Investments: Data-driven insights into funding utilization, including claim metrics and hierarchical analysis of funding source distribution.
- Channel: Multi-dimensional analysis of incentive programs across Solution Provider and Distribution frameworks, incorporating CEI benefit utilization and discount mechanism performance across public sector and growth segments.
- Marketing Campaigns: Granular examination of AWS marketing initiative efficacy, with integrated lead-to-opportunity conversion modeling and funnel progression metrics.
- Training and Certifications: Quantitative assessment of organizational capability development, tracking certifications, accreditation completion rates, and training program progression metrics.

Navigating the Partner Insights dashboards

This section describes the controls, filters, and functions of the Partner Insights dashboard.

Filter by Date – Preset Dropdowns

The Date Filter in Partner Analytics includes two mechanisms to drill down on specific time periods – preset dropdown options based on commonly used time periods, and custom filtering to specific date ranges. Date ranges selected in this filter are automatically applied to all the metrics and tables in the dashboard, as well as to all other dashboards, unless otherwise specified.

Because some metrics in Partner Analytics and Marketplace Insights refresh at different cadences, the preset Date Filter options vary by dashboard.

- Opportunities and Leads have preset dropdown options include Past 30 days, Past 60 days, Past 90 days, Trailing 12 months (TTM), and Year to date (YTD).
- For all other dashboards, preset dropdown options include Past available 1 month, Past available 2 months, Past available 3 months, Year over year (YoY), and Year to date (YTD). Because some metrics do not refresh daily, exact "past X days" filters cannot be applied to these metrics, unlike daily refreshed KPIs. Therefore, dashboard-wide date filters in some dashboards are limited to "Past X available month(s)" dropdown options. The dashboard logic automatically applies relevant date filters to each metric, aligned to the refresh cadences of those metrics. If data

is not available for the current month, the dashboard will source the next most recent month available.

Filter by Date – Custom

In addition to the preset date filters, or set a custom date range. Note that Discounts metrics will still be shown at a monthly level. To specify exact start and end dates:

- Choose 'Custom' in the date filter dropdown menu.
- Click on the 'Start Date' search bar to open a calendar pop-up. Then, choose the desired filter start date in the calendar.
- Repeat Step 2 with the 'End Date' search bar.

Date values for filtering by date:

- The Opportunity date defaults to partner accepted date for AWS Referred Opportunities and Opportunity submitted date for Partner Referred Opportunities
- The Lead date tagging defaults to the created date, regardless of when the Lead was last modified.
- The Investments date defaults to Issued Credit and Redeemed Credit – Promotion Creation Date (the date on which a credit code was generated). All Cash KPIs and Approved Credit – Pre-Approved Date. Discounts follow the billing period.
- The Marketing Campaigns date defaults to campaign-associated data, the Opportunity metrics leverage Opportunity date, the Pipeline reflects Opportunity created date for AO, approval date for PO, the revenue uses Opportunity launch date, and Campaign-associated Leads metrics use Lead date.
- Training and Certifications date defaults to Net New Certification is date of when Certification was awarded for first time (does not include re-certification), Net New Accreditation uses date of course completion, and Net New Training leverages the date of course completion.

At a glance

The 'At a glance' dashboard provides key metrics from each dashboard and now offers visibility into ACE Eligibility and CRM Integration. On this dashboard, filter the data by customizing a start and end date or choosing one of the available options.

This dashboard provides data on the total number of AWS and Partner originated Opportunities and Leads with year-over-year details, as well as the combined cash and credit investments. Finally, view campaign and marketing information if applicable.

Opportunity pipeline analysis

> **Note**
>
> Data is available for download from January 2021 onward.

There are several filters in the Opportunities dashboard to help analyze co-sell pipeline. The below 4 charts respond and adjust based on the filter selections.

Partner Originated Opportunity Trends (TTM):

- Dropdown filter to view the chart by All opportunities, launched opportunities, and validated opportunities. Users can start with the first table in which they can toggle between launched opportunities and partner validated opportunities.
- The total estimated revenue and total number of opportunities with year-over-year details for all opportunities, or broken down to only AWS-originated opportunities, or only partner-originated opportunities.

Opportunity Analysis:

The opportunity analysis allows comparison information on the pipeline, followed by the performance benchmarks. Two identical charts display ACE data for side-by-side comparison. Either a bar chart will be displayed (if over 5 segments exist for the chosen category), or a donut chart will be displayed if 5 or fewer segments exist for the chosen category. The Opportunities By breakdown options are also available as filters for the full Opportunities dashboard.

For information about specific opportunities, leverage the filtering and sorting functionalities seen in the Opportunities Summary Data:

1. Customize the table to only see critical metrics or All Data. Or Filter Displayed Data by just Open Opportunities, only Closed Opportunities, or All opportunities.
2. Drill down to specific Opportunity IDs.

3. Check for operational/data recording discrepancies between the opportunity Stage and the AWS Stage noted by AWS Sellers (mismatches highlighted in red).
4. Sort table columns in ascending/descending order to focus on top priorities.

AWS Engagement Scores:

AWS co-sell recommendation score assesses how well your solutions are positioned to meet current and forecasted customer needs. The High, Medium, and Low scores help you identify your current strengths and opportunities to co-sell with AWS. These scores are currently available to ACE-Eligible partners in Services and Software paths. Scores will not be displayed where we do not have enough data to provide a match and are only available to partners with a specialization.

Opportunities summary data:

In this table, users can see partner stage vs. AWS stage. AWS Stage reflects AWS record keeping in the AWS Seller CRM, while the overall Stage value reflects the opportunity stage in ACE Opportunities page. For Open opportunities, some difference in status recording may be expected due to different systems being updated at different times with manual input. Finally, the user can see the AWS Marketplace Engagement Score and AWS Solution Engagement Score which indicates the likelihood for that customer to buy from AWS Marketplace.

Lead pipeline analysis

The Leads dashboard includes multiple filters to focus on subsets of AWS Lead Referrals, or even specific Leads. In addition to using the Date Filter to drill down on Leads Conversion and Leads Source trends, and leverage the Lead Status filter and filtering on specific Lead ID(s) in the Leads Summary table to dive even deeper:

- **Lead ID:** Multi-select filter to search specific Lead(s) by ID. Enter the desired ID(s) in the search box and select the Lead(s) in filtering the Summary table.
- **Lead Status:** Multi-select filter to slice AWS Lead Referrals by status. Choose a combination of: Select all (all options), Disqualified, Open, Qualified, and Research.

Funding and investments

Please navigate to the funding program for further information.

Resell revenue and discounts

For more information, review the channel partner specific guides: Solution Provider Program & Distribution Program.

Marketing campaign analysis

In addition to the dashboard-wide Date Filter, the Marketing Campaigns dashboard also includes multi-select Filters to parse key AWS Marketing Campaigns metrics by specific Campaign, geographic location (including Geo, Region, and Country filters), as well as AWS Customer Segment and Industry. Except for Campaign, these Filters also apply to metrics on other dashboards that display the same Filters at the top (for example, the Opportunities dashboard).

View summary metrics in the Campaign Summary, with additional metric-specific breakdowns in the visuals below the summary.

Training and certifications

The Training and Certifications dashboard incorporates dual filtering capabilities for analyzing employee achievements:

Category Filter:

- Certification completions
- Accreditation attainment
- Training completion metrics
- Total Addressable Learner population within the organization

Type Filter:

Enables data aggregation through two distinct measurement methodologies:

1. **Total Count:** Measures each completion (Certification, Accreditation, or Training) as an individual unit
2. **Unique Individuals:** Aggregates achievements at the individual level, counting each person as one unit

Example of Measurement Differentiation: For an organization with 10 employees holding 5 certifications each you will see the total count display 50 certifications and unique individuals will display 10 certified individuals.

This filtering system enables precise tracking and analysis of organizational learning achievements through multiple analytical perspectives.

MAP Partner Performance Index (PPI)

The topics in this section explain how to understand and use the MAP Partner Performance Index (PPI). The PPI helps you track your organization's effectiveness in delivering Migration Acceleration Program (MAP) projects and provides insights to improve your migration practice.

> **Note**
>
> Only alliance leads can access the Partner Performance Index dashboard.

Topics

What is the MAP Partner Performance Index (PPI)?

The MAP Partner Performance Index (PPI) is a comprehensive measurement system that evaluates partner effectiveness in delivering successful AWS migration projects where partners have requested investments from AWS. Sustained investment from AWS requires the program to produce an acceptable return on investment, the PPI has been devised to encourage high performers and remediate performance that could negatively impact ROI. PPI provides you with

transparent, data-driven insights into your migration practice performance and helps you identify opportunities for improvement.

Why PPI matters for your business

The PPI helps you build a stronger migration practice by providing transparent, data-driven insights that benefit both your organization and your customers:

For your organization:

- Clear visibility into your migration practice performance
- Identification of specific areas for improvement
- Recognition and rewards for excellence
- Accelerated approval processes for top performers
- Targeted support where you need it most
- Competitive advantage in the marketplace

For your customers:

- Access to proven, high-performing migration partners
- Faster migration completion and value realization
- Higher quality project execution and delivery
- Greater confidence in project outcomes
- Greater attention to the optimized annual costs a customer will incur when running their workloads on AWS

How PPI supports your growth

PPI is designed as a growth tool, not just a measurement system. The mechanism provides you:

- Real-time visibility in your metrics and performance trends which you can use to identify improvement opportunities and improve migration practice
- Based on your opportunities, get targeted support on the specific areas from AWS
- Gain customers trust and through that more business
- An opportunity to have more recommendations from AWS
- Reduce administrative overhead for proven excellence

Understanding your PPI score

Your PPI score is a single percentage that reflects your overall effectiveness across four key performance areas. The score ranges from 33% to 100%, with higher scores indicating stronger performance.

How scoring works

PPI evaluates your performance using four key metrics:

- **Migration Win Rate** – Your ability to convert funded assessments into migration projects
- **Speed to Value** – How quickly you help customers realize value after migration starts
- **Portfolio Success** – Overall revenue achievement across all completed projects
- **Project Success** – Individual project performance and consistency

For each metric, you receive a score of 1, 2, or 3 points based on your performance:

Score	Performance Track	Description
3 points	High Performance Track	Exceeds expectations; demonstrates excellence
2 points	Core Program Track	Meets expectations; solid execution
1 point	Turnaround Track	Below expectations; improvement needed

Your overall PPI score calculation:

PPI Score = (Sum of metric scores) / 12

Example: If you score 2 points on all four metrics: (2 + 2 + 2 + 2) / 12 = 8 / 12 = 67%

> **Note**
>
> If you don't have enough data for a specific metric (for example, too few completed projects), we use the average of your other valid scores to calculate that metric. This ensures new or growing partners aren't unfairly penalized.

Performance tracks

Based on your PPI score, you'll be classified into one of three performance tiers:

Tier	Score Range	Description
High Performance Track	67% - 100%	Partners delivering the strongest results across metrics
Core Program Track	50% - 66%	Partners within core expectations with growth potential
Turnaround Track	33% - 49%	Partners who need support to meet performance standards

The four key performance metrics

This section provides detailed information about each of the four metrics used to calculate your PPI score.

Metric 1: Assess Conversion Rate

What it measures: Your ability to convert AWS-funded Assess projects into signed migration commitments.

How it's calculated:

Win Rate = (Number of Assess-funded Won migrations) / (Number of Assess-funded Won + Lost migrations) in the past 24 months

Performance thresholds:

Performance Level	Win Rate
High Performance Track (3 points)	75% or higher
Core Program Track (2 points)	45% - 75%
Turnaround Track (1 point)	Below 45%

Why it matters:

High conversion rates indicate that you're:

- Effectively qualifying opportunities before requesting funding
- Aligning assessment findings with customer priorities
- Making efficient use of AWS funding resources
- Building strong customer commitment early in the process

How to improve:

- Strengthen your opportunity qualification process
- Ensure thorough customer discovery before submitting funding requests
- Align assessment outcomes with specific customer business drivers
- Maintain regular communication with customers throughout the assessment phase
- Partner closely with AWS account teams during the sales cycle

Example: If you've received Assess funding for 100 projects and 85 of them converted to signed migrations while 15 were lost, your win rate is 85/100 = 85%, earning you 3 points (High Performance Track).

Metric 2: Migration Delivery Velocity Health

What it measures: How quickly your migration projects begin generating meaningful AWS revenue after the project reached $1k in tagged spend.

How it's calculated:

Speed to Value = Percentage of projects reaching $50K within 180 days from $1K date in the past 24 months

Performance thresholds:

Performance Level	Projects Hitting Target
High Performance Track (3 points)	85% or higher of projects
Core Program Track (2 points)	50% - 85% of projects

Performance Level	Projects Hitting Target
Turnaround Track (1 point)	Below 50% of projects

Why it matters:

Fast starts demonstrate that you're:

- Improving Partner Cash Flow by ensuring faster payment of the Mobilize funding
- Effectively planning and executing migration strategies
- Prioritizing high-value workloads early
- Removing blockers and accelerating customer adoption
- Helping customers realize business value quickly

Example: If you have 50 projects that are at least 6 months past their start date, and 44 of them reached $50K within 180 days from the day of $1k, your speed to value is 44/50 = 88%, earning you 3 points (High Performance Track).

Metric 3: Final Migration Revenue Realization on Completed Projects at Portfolio Level

What it measures: Your overall effectiveness in delivering expected revenue outcomes across all completed migration projects.

How it's calculated:

Final Migration Revenue Realization on Completed Projects at Portfolio Level = Sum of tagged spend (MRR) from completed Migrations / Sum of expected terminal ARR from completed migrations in the past 36 months

Performance thresholds:

Performance Level	Revenue Achievement
High Performance Track (3 points)	85% or higher
Core Program Track (2 points)	40% - 85%
Turnaround Track (1 point)	Below 40%

Why it matters:

Strong portfolio performance shows that you:

- Accurately estimate project scope and potential
- Consistently deliver on commitments
- Have effective project management processes
- Maintain customer engagement through project completion
- Solve obstacles/challenges to ensure migration completion

Example: If your completed projects had a combined expected terminal ARR of $10M and you achieved $9.2M in actual map tagged spend, your portfolio success rate is 9.2/10 = 92%, earning you 3 points (High Performance Track).

Metric 4: Final Migration Revenue Realization on Completed Projects at Individual Deal Level

What it measures: The consistency of your project delivery by examining individual project outcomes. This metric prevents a few exceptional projects from masking multiple underperforming ones.

How it's calculated:

Project Success = Percentage of completed projects that achieved at least 50% of expected ARR in the past 36 months

Performance thresholds:

Performance Level	Projects over 50% ARR
High Performance Track (3 points)	70% or higher
Core Program Track (2 points)	31% - 70%
Turnaround Track (1 point)	below 30%

Why it matters:

Consistent project delivery demonstrates:

- Quality execution across your entire portfolio
- Effective risk management and mitigation
- Reliable processes that work for various project types
- Customer satisfaction at the individual project level

Example: If you've completed 30 projects and 26 of them achieved over 50% of their expected ARR, then 26/30 = 87% of your projects met the threshold, earning you 3 points (High Performance Track).

Performance tiers and benefits

The PPI system recognizes different levels of partner capability and provides appropriate support and benefits for each tier.

High Performance Track (67% - 100%)

Who qualifies: Partners delivering exceptional results across all four metrics, or strong performance in most areas.

Strategic benefits:

- Enhanced funding eligibility for large or strategic projects
- Featured partner status in AWS partner programs
- Opportunity to showcase your success in AWS marketing materials

Recognition:

- In future, ability to promote your Top Performer status publicly
- Inclusion in AWS partner success stories
- Priority consideration for AWS Competency programs
- Featured in Partner Matching Engine for AWS-originated opportunities

Support:

- Regular business reviews with AWS Partner Development Managers
- Invitations to exclusive partner events and roundtables

Core Program Track (50% - 66%)

Who qualifies: Partners meeting core expectations with solid execution and clear growth potential.

Core benefits:

- Standard funding access for qualified opportunities
- Regular technical support and program resources
- Established approval processes and service levels
- Access to AWS migration tools and frameworks

Development benefits:

- Performance improvement guidance and consultation
- Best practice documentation and enablement resources
- Regular business reviews with Partner Development team
- Access to training and certification programs
- Targeted support in specific areas for improvement

Support:

- Standard AWS Partner support channels
- Access to migration best practices and playbooks
- Partner community forums and knowledge base
- Quarterly performance reviews

Focus areas:

If your performance falls in the lower end of this range (50-55%), AWS will work with you to identify specific improvement opportunities and provide targeted resources to help you advance to the next tier.

Turnaround Track (33% - 49%)

Who qualifies: Partners who need focused support to meet performance standards. This tier is designed to help you succeed through targeted resources and guidance.

Support benefits:

- Get to Green (GTG) improvement plan – Work with AWS to create a structured improvement plan with clear, achievable goals
- Dedicated improvement planning with specific, measurable targets
- Enhanced project oversight and guidance
- More frequent check-ins and business reviews (bi-weekly or monthly)

Path to success:

- Clear, time-boxed performance targets
- Regular progress reviews to track improvement
- Focused enablement support and training
- Access to top performer best practices and case studies
- Dedicated Partner Development Manager support

During the improvement period:

You'll continue to have access to MAP funding while actively working on your improvement plan. The improvement period is time-boxed, and your active projects provide opportunities to improve your metrics in real-time.

What we ask:

- Commitment to the improvement plan
- Regular participation in progress reviews
- Cooperation in maintaining data accuracy and timely project updates
- Implementation of recommended best practices

Using the PPI dashboard

The PPI dashboard provides real-time visibility into your performance metrics and trends. This section explains how to access and use the dashboard effectively.

Accessing the dashboard

To start the PPI dashboard:

1. Sign in to AWS Partner Central as an alliance lead.
2. Open the Dashboards list and choose the Migration Partner Performance Index analysis in the left panel.

> **Note**
>
> Currently, only users with the alliance lead role can access the PPI dashboard. We're working to expand access to other roles in future releases.

Dashboard sections

The PPI dashboard contains the following key sections:

1. Migration summary data

- Your overall PPI score
- Current performance tier
- Total won ARR (Active and Completed projects)
- Total project count
- Data freshness indicator

2. Key metrics overview

- Current score for each of the four key metrics
- Point values (1, 2, or 3) for each metric
- Visual indicators (color-coded performance)
- Trend indicators showing improvement or decline

3. Contributing metrics detail

- Underlying data used to calculate each key metric
- Actual numbers and percentages
- Comparison to performance thresholds

4. Historical trends

- Month-over-month performance changes
- Trend lines for each metric
- Identification of improvement patterns

Filtering your data

You can customize your dashboard view using the following filters:

Display data by:

- Current monthly score – Your most recent performance snapshot
- Historic monthly view – Line graph showing 12 months of performance trends

Opportunity type:

- All MAP 2.0 projects
- MAP only (excludes MAP Lite)
- By program type

Customer Geography (PPI score will continue to be at the global level):

- All geographies
- NAMER (North America)
- EMEA (Europe, Middle East, Africa)
- APJ (Asia Pacific & Japan)
- LATAM (Latin America)

Understanding your dashboard data

To interpret your metrics:

1. Review your overall PPI score – This is your primary indicator of performance.
2. Examine individual metric scores – Identify which areas are strong and which need attention.
3. Check contributing metrics – Understand the underlying data driving each score.

4. Review historical trends – Look for patterns and the impact of improvement efforts.
5. Compare to thresholds – See how close you are to the next performance tier.

Example interpretation:

Overall PPI Score: 75%

- Migration Win Rate: 3 points (85% conversion)
- Speed to Value: 2 points (72% of projects hit target)
- Portfolio Success: 3 points (95% revenue achievement)
- Project Success: 2 points (25% of projects below 50%)

Interpretation: You're a Top Performer overall, with particular strength in win rate and portfolio-level execution. Focus on improving speed to value and project consistency to reach 100%.

Dashboard refresh frequency

- PPI scores are calculated monthly
- Data is refreshed on the 1st of each month
- Historical data is available for the past 12 months
- Real-time project data may take 2-3 business days to reflect in PPI calculations

How to improve your PPI score

This section provides actionable strategies to improve your performance in each metric area.

General best practices

Data accuracy is critical:

- Ensure all project data in MPE (Migration record that AWS tracks internally) is accurate and up-to-date
- Provide realistic, well-justified ARR estimates in funding requests
- Update project start and end dates promptly when circumstances change
- Properly tag all migrated workloads for accurate revenue tracking
- Report project status changes as they occur

Leverage AWS resources:

- Work closely with your Partner Development Manager (PDM)
- Attend AWS migration best practice sessions
- Use AWS migration frameworks and tools
- Participate in partner enablement programs
- Learn from top performer case studies

Maintain customer focus:

- Keep customers engaged throughout the migration lifecycle
- Conduct regular business value reviews
- Address blockers and challenges proactively
- Ensure customer success is the primary goal

Preparing for PPI

What you can do now:

- Review your data – Ensure all project information in MPE is accurate and up-to-date
- Understand the metrics – Familiarize yourself with the four key performance areas
- Assess your practice – Honestly evaluate where you might need improvement
- Engage with AWS – Work with your PDM to prepare for PPI
- Clean up attribution – Correct any projects incorrectly attributed to your organization
- Update training – Ensure your teams understand MAP 2.0 requirements and best practices

Getting help and support

Access AWS Partner Central resources

1. Sign in to AWS Partner Central
2. Navigate to Support → Contact Support
3. Choose Partner Programs as your topic
4. Select MAP Performance Index as the issue type

Submit data correction requests

Work with your PDM to submit corrections for:

- Project attribution errors
- Incorrect project dates
- ARR estimate updates
- Project status discrepancies

Attend enablement sessions

AWS hosts regular enablement sessions on:

- Migration best practices
- PPI optimization strategies
- New program features
- Top performer insights

Check the AWS Partner Central events calendar for upcoming sessions.

Contact your Partner Development Manager (PDM)

Your PDM is your primary point of contact for all PPI-related questions and support. They can:

- Help you understand your PPI score and metrics
- Provide improvement recommendations
- Assist with data corrections and validation
- Connect you with technical resources
- Answer questions about program policies

Additional resources

- AWS Migration Acceleration Program (MAP) Overview: [Partner Central Link]
- Migration Best Practices: [Partner Central Link]
- AWS Migration Tools and Services: [AWS Link]

- Partner Development Manager Directory: [Partner Central Link]
- Partner Analytics Dashboard: AWS Partner Central → Analytics & Insights

Summary

The MAP Partner Performance Index represents AWS's commitment to data-driven partner development and customer success. By providing transparent, actionable performance insights, PPI helps you:

- Understand where your migration practice excels and where it can improve
- Access the right level of support and resources for your needs
- Demonstrate your expertise to customers and AWS teams
- Grow your migration practice with confidence

Success in PPI comes from:

- Accurate data and realistic commitments
- Customer-focused execution
- Continuous improvement mindset
- Partnership with AWS teams
- Consistency across your entire project portfolio

AWS is committed to your success. The PPI program is designed to help you build a world-class migration practice that delivers exceptional outcomes for customers.

For questions or support, contact your Partner Development Manager or AWS Partner Support.

Attributed Revenue

The Attributed Revenue dashboard provides visibility into the AWS revenue impact of your solutions as measured by Partner Revenue Measurement (PRM). The dashboard displays aggregated revenue tracked by PRM capabilities across all customers at a monthly grain, broken down by product and AWS service.

For more information, review the Partner Revenue Measurement Guide and FAQs.

Filters

The Attributed Revenue dashboard incorporates the following filtering capabilities for analyzing your attributed revenue data:

- **Time Frame:** Select a date range to view attributed revenue for specific billing periods.
- **Product Name:** Filter by one or more of your AWS Marketplace product listings to view revenue for specific products.
- **AWS Service:** Filter by specific AWS services (for example, Amazon EC2, Amazon S3, Amazon RDS) to understand which services your solutions drive consumption for.
- **AWS Account ID:** Filter by specific AWS account IDs to view revenue associated with particular accounts.

Key metrics

The dashboard displays three key metrics at the top of the page:

- **Products Measured:** The number of your AWS Marketplace products that have attributed revenue tracked by Partner Revenue Measurement during the selected time frame.
- **AWS Services Measured:** The number of distinct AWS services where your products are driving consumption during the selected time frame.
- **Total Attributed Revenue:** The total aggregated revenue measured by Partner Revenue Measurement across all your products, services, and customers during the selected time frame.

Charts

Attributed Revenue by Product

This chart displays month-over-month attributed revenue for each of your AWS Marketplace products. Each product is represented as a separate series, allowing you to compare revenue trends across your product portfolio over time. Use this chart to identify which products are driving the most AWS consumption and track growth patterns.

Attributed Revenue by AWS Service

This chart displays attributed revenue broken down by AWS service. Use this chart to understand which AWS services your solutions drive the most consumption for and how service-level revenue trends change over time.

Tables

Attributed Revenue

This table shows revenue tracked by Partner Revenue Measurement capabilities aggregated across all customers at a monthly grain. The table includes the following columns:

- **Product Name:** The name of your AWS Marketplace product.
- **AWS Service:** The AWS service where consumption was measured.
- **Billing Month:** The month for which revenue was measured.
- **Attributed Revenue:** The aggregated revenue amount for the product-service-month combination.

Revenue data is aggregated across all customers and is only displayed when a product is consumed by a minimum threshold of unique customer accounts per month. Individual customer revenue, names, or account IDs are not displayed.

Onboarding Status

This table shows your products that AWS can see enabled with any of the Partner Revenue Measurement capabilities. Use this table to verify that your PRM implementation is active and to identify products that may need additional configuration. The table displays:

- **Product Name:** The name of your AWS Marketplace product.
- **PRM Capability:** The Partner Revenue Measurement capability enabled for the product — Resource Tagging, User Agent string, or AWS Marketplace Metering.
- **Status:** Whether the capability is actively tracking revenue for the product.

Data availability and privacy

- Revenue data is refreshed monthly and reflects the previous billing month's consumption.
- Revenue is only displayed when a product is consumed by a minimum threshold of unique customer accounts per month. If the customer count drops below the threshold for any month, no revenue data is displayed for that product for that month.
- Partners receive only aggregated revenue data at the product and service level. Individual customer revenue, names, or account IDs are never shared.

- Internal AWS accounts and accounts generating $0 in AWS revenue are excluded from threshold calculations.

Prerequisites

To access the Attributed Revenue dashboard, you must:

1. Be on the new AWS Partner Central experience (PC 3.0).
2. Have implemented at least one Partner Revenue Measurement capability — Resource Tagging, User Agent string, or have an AMI or ML product listed on AWS Marketplace (for automatic Marketplace Metering).

Partners with subsidiary accounts connected via Partner Account Connections (PAC) will see aggregated revenue across all connected accounts in a single view.

Learn more

- Partner Revenue Measurement Onboarding Guide
- Resource Tagging Implementation
- User Agent String Implementation
- AWS Marketplace Metering

Export (Download) Data

The ability to export the data displayed in a visual to a downloadable CSV/Excel file is available.

> **Note**
>
> Only data from 2021 will be available to download. The tool does not support raw data download, only the data displayed within the table, and this feature is not supported on every table within the dashboard.

To export data:

1. Hover over to the top right corner of any chart or table to locate 3 vertical dots
2. Select the 3 vertical dots

3. From the drop down select Export to CSV
4. The data will be formatted as displayed on the dashboard.

Data Refresh and Denominations

The dashboard data refreshes on the following specified cadences:

- **Daily**
  - ACE data
  - Marketing Campaigns data
  - Leads data [approximately 2PM (PST) every day]
  - Investments data; Credits and Cash KPIs refresh one to four times daily.
  - Training and Certifications data refreshes once a day.
- **Monthly**
  - Discount KPIs on the 15th day of each month.

Seller Insights Dashboard

AWS Marketplace provides dashboards powered by Amazon QuickSight with charts, graphs, and insights that help you access and analyze financial, sales, and marketing data. For information about specific dashboards available, see here.

Dashboards are available to AWS Marketplace sellers who have the appropriate permissions. For more information, see AWS managed policies for AWS Partner Central.

Partner Analytics and Seller Insights Frequently Asked Questions (FAQs)

Review the below FAQs for answers to common questions.

General FAQs

'No Data' is displayed on any of the KPIs, how do I fix this issue?

Please select the reset button (circular arrow). Note, this is different from the refresh button on the web browser page.

I see there are data discrepancies? What do I do?

File a ticket with APN Support to resolve discrepancies. From the left navigation panel, choose AWS Partner Central support to file a ticket.

Why doesn't the Partner Scorecard data match what is shown in Partner Analytics dashboard data?

Data discrepancies between Partner Analytics and the Partner Scorecard stem from several key differences in measurement methodologies and scope. The Scorecard's measurement period aligns with the organization's last tier review date, creating potential mismatches when date filters differ. Additionally, the Scorecard maintains broader inclusivity by counting all opportunities where partners are tagged in AWS internal systems, regardless of entry status. Training and Certification data variations occur as the Partner Scorecard specifically tracks progress within selected Partner Paths, focusing on Unique Individuals with Foundational, Technical Certifications, and Business/Technical Accreditations. Partner Analytics provides expanded functionality through comprehensive achievement tracking, including Total achievement counts via Type filtering, Level-based certification aggregation rather than technical definitions, and inclusion of non-APN Tier requirement credentials including the AWS Partner: Cloud Economics accreditation, which remains absent from the Partner Scorecard.

Opportunities dashboard FAQs

Why does the Opportunity Win Rate visual show a different count of Launched and Closed Lost opportunities (and a different Win Rate) than the count displayed on the Opportunities Analysis bar chart split by Stage?

Opportunity win rate metrics are calculated based on the Close Date of opportunities (date an opportunity launches or becomes Closed Lost) and so includes all opportunities closed within the selected timeframe, regardless of when they were submitted. The Opportunities Analysis bar chart is filtered by the opportunity Submitted date (close dates do not exist for opportunities still open), so the Launched and Closed Lost opportunity counts shown in the Opportunities Analysis only include opportunities submitted within the selected timeframe.

Why does the Partner Referrals Approval Rate visual show a different count of Approved and Rejected opportunities than the count displayed on the Opportunities Analysis donut chart split by Status?

Partner Referrals Approval Rate metrics are calculated based on the date opportunities are approved/rejected and so includes all opportunities approved within the selected timeframe, regardless of when they were submitted. The Opportunities Analysis bar chart is filtered by the opportunity submitted date, so Approved and Rejected opportunity counts shown in the Opportunities Analysis only include opportunities summitted within the selected timeframe.

Why are Stage and AWS Stage values different for some opportunities?

AWS Stage reflects AWS record keeping in the AWS Seller CRM, while the overall Stage value reflects the opportunity stage in the ACE Opportunities Page. If these two values are different for an opportunity Closed at least 48 hours earlier, please reach out to the AWS Partner Development team to resolve any operational/record-keeping discrepancies. For Open opportunities, some difference in status recording may be expected due to different systems being updated at different times with manual input.

AWS Co-sell recommendation score FAQs

How do I see AWS Co-Sell Recommendation Scores on Partner Analytics?

This feature is currently available to ACE-Eligible Partners in AWS Specialization programs.

How does the recommendation logic work?

The recommendation logic is powered by machine learning that is trained on partner capabilities using a predictive model that evaluates these attributes to assess the best-fit partners by geography, industry, size, and capability. The recommendation score assesses the likelihood of success in engaging with AWS for co-sell.

What do I need to do to receive a higher score?

For Services path partners, the key is providing high-quality, detailed information in the opportunity record. Ensure that the entire pipeline in ACE and that opportunity details are up to date. Opportunity hygiene should include opportunity details: opportunity title should include a summary of the project [customer name, workload, delivery], a detailed description of the customer use case (a few short sentences are better than lengthy filler), business outcome includes desired end result of the AWS Customer, include next steps and update this as more information

is acquired, true estimated or exact opportunity value. Ensure that any relevant AWS services used to deliver the opportunity are listed in the opportunity text fields (e.g., Description) and provide quality over quantity of information.

For Software path partners, Marketplace Solution Listings are used within the algorithm, so ensure hygiene of the solution listing and up to date information. Attach a solution listing to ACE opportunities (link the marketplace listing to any relevant opportunities) and try to process deals through Marketplace for higher recommendations.

How does AWS Marketplace influence my recommendations?

For Software path partners, a public AWS Marketplace listing is a necessary condition to be evaluated by the model. The model uses the product category, product description, and current customer deployments to evaluate where the listing can meet AWS customer needs. The more data we can gather with the listing and customer activity, the more likely the listings will be recommended.

How does the model evaluate my capabilities? What do I need to focus on?

For Services path partners, the model uses the following fields from the opportunity record: Title, Description, Details, Need, Next Step, and Value. The model can also derive capabilities based on AWS Product tags. To evaluate where partners are well-suited for co-selling, the model inspects open AWS customer opportunities and predicted customer use cases, to find partners that have demonstrated success with similar customers.

For example, the model currently runs upon all open AWS Originated (AO) opportunities. For each given customer account and opportunity, the model predicts the partner based on their past success delivering with similar customers and use cases. Where available, the model will return to partners that have done work in the same region, segment, and/or industry.

How do Service Validations, Competencies, and Programs affect my recommendation score?

AWS Co-Sell Recommendation Scores are provided as a benefit for ACE Eligible and AWS Specializations partners. Service Validations and AWS Competencies with corresponding ACE launches provide the model with confidence about partners' capabilities. The model also use validated case studies, either to improve recommendation relevance or to provide additional explanation for why a recommendation was made. This means that partners with validated and published case studies can potentially see shifts in their recommendation scores.

What if the wrong use case was tagged to my opportunity?

An update can be made to open opportunities only, per ACE guidelines. The machine learning model is re-trained weekly to capture new data on launched opportunities and marketplace offers. Ensure that the information is accurate before moving the PO or AO to "Launched" state.

Should I submit more opportunities, including for-visibility-only (FVO) with no co-sell support?

Yes. The model is enriched as partners share more data about their capabilities.

How does win rate, deal size, and solution data impact recommendations?

A minimum of one high quality launched deal (Partner Originated or AWS Originated) is required by the model. Additional high quality opportunity submissions (or referrals) will strengthen the connection between customers, their needs, and capabilities. Follow the guidelines outlined earlier in this doc to maximize data quality.

I am ACE-Eligible and AWS Specialized, but only see "Low" or no scores?

For Software Path Partners:

1. Have at least 1 Marketplace listing in any category, except for ProServe, and
2. Have lifetime EC2+GSS (private offers or public subscriptions) over $100, and

For Services Path Partners:

1. Include relevant AWS Product tags and/or keywords in the description
2. Submit more opportunities in areas that are specialized.

If a score still doesn't populate, it is also possible that we have not identified current / potential customer use cases that match the partner's capabilities.

I am ACE eligible and have submitted 100's of POs but received no AWS Co-Sell Recommendation Score. Why?

Data quality supersedes quantity in all documentation processes. Strict adherence to established guidelines ensures optimal system performance through accurate customer problem

documentation and precise AWS service implementation details. Critical documentation parameters must include specific technical solutions, deployed AWS services in designated fields, and accurate opportunity valuations. When addressing specialized customer challenges, detailed documentation of technical implementations and solution architectures enables the AWS Co-Sell Recommendation Score to establish precise connections between solutions and future opportunities.

As a Software partner, do I need a public AWS Marketplace listing to be included in the model?

Yes and No. AWS Marketplace Listings is currently the primary source used by the model to evaluate Software path partner capabilities. The model supplements this data with ACE opportunity launches for Software partners.

As a Services partner, do I need a public listing on Marketplace to be recommended?

Not currently.

AWS Marketplace Engagement Score FAQs

What is the AWS Marketplace solution engagement score?

The AWS Marketplace solution engagement score predicts a customer's likelihood to purchase a solution from a partner. The output of the model is a probability that demonstrates the likelihood for the customer to need a solution from the partner. These probabilities are transformed into HIGH / MEDIUM / LOW / "-" groupings.

How do I act on the AWS Marketplace Engagement Score?

AWS Marketplace streamlines procurement and onboarding processes, creating significant value for customer purchasing workflows. The AWS Marketplace Engagement Score serves as a prioritization tool for identifying opportunities aligned with marketplace procurement preferences. While the score provides directional insights, it does not guarantee transaction outcomes through AWS Marketplace. Optimization of co-sell opportunities requires direct engagement with the AWS Partner Development team for strategic prioritization and execution planning. The scoring mechanism functions as one component within a comprehensive evaluation framework, supporting data-driven decision-making while acknowledging the dynamic nature of customer purchasing behaviors and preferences.

Many of my opportunities show "-" for the AWS Marketplace Engagement Score?

The "-" value indicates that AWS was either 1) Unable to determine the AWS Marketplace Engagement Score for that opportunity based on currently available information; or 2) Unable to assign an AWS Marketplace Engagement Score, as it is not applicable for that opportunity. This flag is only available for partners registered on the AWS Marketplace, as it covers AWS Marketplace listings.

I am listed on AWS Marketplace, but I do not see AWS Marketplace Engagement Scores for my opportunities?

First ensure that the Display AWS Marketplace Engagement Score filter is set to Yes in the Opportunities Summary Data table in the Opportunities dashboard of Partner Insights. If there is an issue still, reach out to APN Support for help resolving this issue.

What does HIGH/MEDIUM/LOW mean?

High means a customer's likelihood of purchasing a solution rank among the top cohort in comparison with all other customers. Medium means a customer's likelihood of purchasing a solution rank in the middle of the cohort in comparison with all other customers. Low means a customer's likelihood of purchasing a solution rank below the median in comparison with other customers.

Does AWS Marketplace solution engagement score surface for all partners and opportunities?

No. AWS Marketplace solution engagement scores like Marketplace engagement scores are only relevant to independent software vendors (ISV) or Software path partners with Marketplace listings.

What is the difference between AWS Marketplace engagement and AWS Marketplace solution engagement?

AWS Marketplace engagement score predicts a customer's likelihood to purchase through the AWS Marketplace. The AWS Marketplace solution engagement score is a score that predicts a customer's likelihood to purchase a solution from the partner's solution listing. One is about the procurement channel, and the other is about solution procurement.

How frequently are AWS Marketplace solution engagement scores updated?

Monthly.

Why do I see different scores on each opportunity? Why does the Marketplace engagement score not match the AWS Marketplace solution engagement score?

While a customer may have a high likelihood to make a purchase through the AWS Marketplace, this does not mean a customer has a high likelihood to purchase a partner solution and vice versa.

Does a higher Solution engagement score mean that a customer is already using this solution through similar services or my competitors?

No. The Solution engagement score protects customer confidentiality and partner data. The score reflects a comparative ranking relative to other customers. A HIGH score indicates the customer's potential alignment with the solution, not their current service usage with AWS or other providers.

Can I see the score for both AWS originated and Partner originated opportunities?

Yes, Technology partners can view the AWS Marketplace solution engagement score for both AWS originated (AO) and Partner originated (PO) opportunities.

Does a higher score mean that a customer has an EDP, purchased from AWS Marketplace already or has a higher spend on AWS?

No, The Solution engagement score is derived in a way to protect customer confidentiality. A HIGH score indicates the customer's potential alignment with the solution, not their confidential enterprise agreement, current service usage with AWS, or other providers.

Marketing Campaigns FAQs

I see more campaigns on the donut charts for Leads shared by campaign, Opportunities by campaign, ARR by campaign than the total active campaigns?

The donut chart of Leads shared by campaign shows all the leads shared with the filtered time period and the contributing campaigns can be from the same time period and prior. For example, when filtering on 2023YTD, a portion of leads shared within 2023YTD can be from campaigns run in 2022. Same reason applies to Opportunities by campaign and ARR by campaign donut charts.

Why are some identically-named metrics in the Marketing Campaigns dashboard showing different values from metrics with the same name in other dashboards?

Metrics in the Marketing Campaigns only show data associated with AWS-led marketing campaigns, so values indicated may only be a subset of the same metrics shown in other dashboards. For example, opportunity counts in the Marketing Campaigns only show opportunities generated from AWS-led marketing campaigns, while the Opportunities dashboard will show all of the ACE opportunities.

Training and Certifications FAQs

Our records of certified, accredited, and/or trained individuals do not match what is shown in the Training and Certifications dashboard?

The Training and Certifications dashboard only includes data for individuals that have either 1) Achieved/completed the Certification, Accreditation or Training using a company email address whose domain is listed in their companies domains in the Training and Certification tab of AWS Partner Central Settings; or 2) Have associated the personal email address they used to achieve or complete the Certification in the AWS Training and Certification badges section of their Profile in Skill Builder. Which email they use and associated actions must be selected or taken by the individual and cannot be completed by AWS or someone else in the organization. Training and Certification totals will change if users merge company email-based profiles with other profiles or if they associate their personal email with a different employer.

AWS Partner Central PII Certifications table does not match what is shown in the Training and Certifications dashboard?

The Personal Identifiable Information (PII) certification table in AWS Partner Central is updated through a different process because of its inclusion of PII information. The cadence of this process could cause a mismatch to what's shown in Partner Analytics, which is updated on a daily basis.

CRM Integration

AWS Partner Central enables CRM integrations, which helps Partners and AWS jointly track customer interactions, manage leads, and streamline sales processes directly within their existing CRM workflows. This integration enables automatic data synchronization between AWS Partner Central and a partner's CRM system. For more information, see AWS Partner CRM integration.

Topics

Mapping AWS Marketplace roles to a CRM integration user

This section explains how to map AWS Marketplace AWS Identity and Access Management (IAM) roles to your CRM integration service user on AWS Partner Central. Mapping enables the CRM Integration service user to perform actions on the AWS Marketplace account. Selecting an IAM role to access AWS Marketplace APIs through CRM integration enables features such as linking AWS Marketplace private offers to ACE opportunities.

Before mapping, you must first complete the following:

- Create IAM roles in the AWS Marketplace account.
- While creating IAM roles, add the following custom trust policy to allow AWS Partner Central to map the IAM roles.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "partnercentral-account-management.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
```

```
}
```

- Grant permissions to perform the `ListEntities` and `SearchAgreements` actions. For more information, refer to Controlling access to AWS Marketplace Management Portal.
- Link your AWS Partner Central account to an AWS Marketplace account.

To map an AWS Marketplace IAM role to a CRM integration user

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **AWS Marketplace** section of the AWS Partner Central homepage, choose **Manage Linked Account**.
3. On the **AWS Marketplace page**, in the **IAM role for CRM integration** section, choose **Map IAM role**.
4. Choose an IAM role from the dropdown list.
5. Choose **Map role**.

To unmap an AWS Marketplace IAM role from a CRM integration user.

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **AWS Marketplace** section of the AWS Partner Central homepage, choose **Manage Linked Account**.
3. On the **AWS Marketplace page**, in the **IAM role for CRM integration** section, choose **Unmap IAM role**.

Logging AWS Partner Central API calls with AWS CloudTrail

AWS Partner Central is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Partner Central. CloudTrail captures calls from the AWS Partner Central console and code calls to the AWS Partner Central API operations as events.

CloudTrail is active in your AWS account when you create it and doesn't require any manual setup. Supported event activity in AWS Partner Central is recorded in a CloudTrail event, along with other AWS service events, on the **Event history** page of the CloudTrail console. There you can view, search, and download events in your AWS account.

Every event or log entry contains the identity of the user who generated the request. This information helps you determine if the request was made by any of the following:

- A user with root or AWS Identity and Access Management user credentials.
- A user with temporary security credentials for a role, or a federated user.
- Another AWS service.

AWS Partner Central supports logging the `partnerCentralAccountManagement` operation as events in CloudTrail log files with `eventSource` `partnercentral-account-management.amazonaws.com`

Topics

AWS Partner Central log file entry examples

Example: `AssociatePartnerAccount`


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"EX_PRINCIPAL_ID",
      "arn":"arn:aws:iam::123456789012:user/Alice",
      "accountId":"123456789012",
      "accessKeyId":"EXAMPLE_KEY_ID",
      "userName":"Alice"
   },
   "eventTime":"2023-10-11T20:57:35Z",
   "eventSource":"partnercentral-account-management.amazonaws.com",
   "eventName":"AssociatePartnerAccount",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"192.0.0.2/24",
   "userAgent":"Mozilla/5.0",
   "requestParameters":{
      "value":"HIDDEN_DUE_TO_SECURITY_REASONS"
   },
   "responseElements":null,
   "requestID":"F9PAD7MAYFGV73S4T7B3",
   "eventID":"fe2a5873-773c-462a-b7c8-810d224de821",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
   "recipientAccountId":"123456789012",
   "eventCategory":"Management"
}
```

Example: `DisassociatePartnerUser`


```
{
   "eventVersion":"1.09",
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"EX_PRINCIPAL_ID",
      "arn":"arn:aws:iam::123456789012:role/PartnerCentralRoleForCloudAdmin-1234",
      "accountId":"123456789012",
      "accessKeyId":"EXAMPLE_KEY_ID",
      "invokedBy":"partnercentral-account-management.amazonaws.com"
   },
   "eventTime":"2023-10-11T20:57:35Z",
   "eventSource":"partnercentral-account-management.amazonaws.com",
   "eventName":"AssociatePartnerUser",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"partnercentral-account-management.amazonaws.com",
   "userAgent":"partnercentral-account-management.amazonaws.com",
   "requestParameters":{
      "partnerUserId":"005123456789012345",
      "iamRoleArn":"arn:aws:iam::123456789012:role/PartnerCentralRoleForUser-1234",
      "partnerAccountId":"1234567"
   },
   "responseElements":null,
   "requestID":"655832a6-8452-4088-9a0f-17212fa55765",
   "eventID":"f7394769-4a3b-4101-9b00-ee0b86a77d89",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
   "recipientAccountId":"123456789012",
   "eventCategory":"Management"
}
```


Related topics

For more information, refer to the following sections in the AWS CloudTrail User Guide:

- Creating a trail for your AWS account
- AWS service integrations with CloudTrail logs
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions

- CloudTrail userIdentity element

Managing AWS subsidiary account connections

From Account Connections, you can manage connections between your own partner or seller accounts. For example, you have multiple AWS Marketplace Seller Accounts, you want to connect with your Partner Account.

Key Concepts

Primary Account

The primary account is an account where you're registered as both a partner and seller. Use this account for administration purposes and to send connection requests.

Connected Accounts

Seller accounts that you own and want to connect with or have connected to your primary account.

Accessing Account Connections

To access Account Connections:

1. Sign into AWS Partner Central.
2. From the left navigation panel, select click on the left side panel and then select Subsidiary Account Connections.

> **Note**
>
> In order to send connection requests to any new account, you need to be logged into your primary account.

Sending Connection Requests to Your Own Seller Accounts That You Want To Connect With Your Partner Account

Once you are in Primary account and in the Subsidiary Account Connections page, you can view all the accounts that you own and are already connected. To connect new accounts:

1. Click on **Send connection request**.
2. Fill out the connection request form with:
   - Your full name
   - Your email address
   - 12-digit AWS account IDs of the accounts that you own and want to connect with
3. Review your selections.
4. Confirm all accounts added in the selected account table.
5. Click on **Send connection request**.

A connection request is sent to each account in the table.

> **Note**
>
> If you need help to know your AWS Account ID, refer to https://docs.aws.amazon.com/accounts/latest/reference/manage-acct-identifiers.html.

> **Important**
>
> Only connect accounts that you own (for example, AWS Marketplace seller accounts). Do not add accounts owned by other partners.

Accepting Connection Requests

To accept connection requests, you need to log into your subsidiary accounts that you sent the connection request to. For each account:

1. Sign in to AWS Partner Central.
2. In the left navigation pane, choose Subsidiary Account Connections.
3. Choose the Connection Requests tab and navigate to Connection Requests.
4. Select the connection request from your primary account.
5. Click **Accept** to connect with your primary account.

To decline: Choose **Reject** instead of **Accept**.

View and Manage Connected Accounts

To view and manage all your connected Accounts:

1. Sign in to your primary account AWS Partner Central.
2. Navigate to the Subsidiary Account Connections page.
3. View the Account Connections tab to see all accounts connected with your primary account.

Getting Help

For additional support with Partner Discovery, Partner Connections, and Account Connections:

- Contact AWS Partner Support through your AWS Partner Central account
- Access the Partner Central Help Center for detailed documentation
- Reach out to your Partner Development Manager (PDM) for guidance
- Join Partner Central community forums for peer support

Migrating to Partner Central in the AWS Console

Existing APN Partners will be provided with a self-service migration tool from within their legacy Partner Central account. Upon completing migration pre-requisites, partners can use the tool to schedule and complete their migration.

Migration process

The migration process consists of four steps:

1. **Review all pre-migration readiness steps in the checklist below.**
2. **Link an AWS account to you APN account (if not yet completed).** The linked AWS account will be charged for the APN Membership Fee and will become the primary account for managing all AWS-related activities. For more information, see Linking AWS Partner Central and AWS accounts. Upon migrating, accessing Partner Central will be through the linked AWS account, where partner users will need the appropriate IAM roles and permissions to gain access. This means users will authenticate through the linked AWS account using their assigned IAM credentials to access Partner Central features and capabilities. See Accessing Partner Central for more details.
3. **Set up user access through AWS IAM, including assigning new managed policies to control access to Partner Central features.** See instructions below for user onboarding during migration.
4. **Schedule or initiate migration.** Users assigned as the alliance lead or cloud admin roles in the legacy Partner Central environment can access the self-service migration tool to select the preferred migration date and time. Once scheduled, alliance leads should alert all active Partner Central users of the scheduled date and time. Once the migration is initiated, all users will be blocked from accessing Partner Central. As a result, we recommend scheduling the migration during non-business hours. The migration typically takes between 2 to 6 hours, depending on the amount of data required to transfer. Upon successful migration, alliance leads will be notified via email and all users will be able to log into the new Partner Central experience with their new IAM credentials.

User onboarding during the migration process

Step 1: Determine permissions for users

1. From the AWS Partner Central homepage, select **View Instructions** in the migration widget.
2. Follow the step-by-step instructions outlined in the tool.
3. Choose **Download Partner Central users**.
4. Open downloaded file of existing users. Based on their current Partner Central role assignment, and attributes such as Last Login Date, determine which users are required to be onboarded in the new Partner Central experience.
5. Map users to specific IAM managed policies based on their current role assignment. Refer to AWS managed policies for AWS Partner Central users for mapping and managed policy documentation.

> **Note**
>
> Users who only require access to Skill Builder for AWS training and certification content will no longer need access to AWS Partner Central. For more information, see Associating domains to your AWS Partner Central account.

Step 2: Work with your IAM Administrator to determine the appropriate onboarding option for users with managed policies

The IAM Administrator should assign the appropriate managed policies to each user according to the mapping above. The process of onboarding users to IAM depends on a partner's AWS account access setup. Refer to Controlling access for AWS Partner Central users for more information.

Linking AWS Partner Central and AWS accounts

AWS recently updated the AWS Partner Central Network (APN) fee policy. The change requires partners to link an AWS account to their AWS Partner Central account in order to confirm their AWS Partner Network (APN) membership. The linked AWS account becomes the primary account for managing Partner Central engagements and activities, including APN fee billing, solutions

management, and APN Customer Engagement (ACE) opportunity tracking using the Partner Central APIs.

You must link to an AWS account that has the IAM roles and permissions needed to access Partner Central.

Account linking has other benefits:

- You can use Partner Connections to work on co-selling deals with other partners to progress deals faster and expand your reach. For more information, see Partner connections in the AWS Partner Central Sales Guide.
- You can use the AWS Partner Central API to integrate Partner Central with your CRM system. Integration synchronizes engagements, opportunities, solutions, and real-time event notifications. For more information, refer to AWS Partner CRM integration in the AWS Partner CRM Integration Guide.
- If you're an ACE eligible partner who links to an AWS Marketplace seller account, AWS Demand Generation Representatives pre-qualify leads from AWS Marketplace and transfer validated AWS originated opportunities to you.

The following topics explain how to link accounts.

- Prerequisites
- Linking AWS Partner Central and AWS accounts
- Unlinking AWS Partner Central and AWS accounts
- Account linking FAQ

Linking AWS Partner Central and AWS accounts

AWS recently updated the AWS Partner Central Network (APN) fee policy. The change requires partners to link an AWS account to their AWS Partner Central account in order to confirm their AWS Partner Network (APN) membership. The linked AWS account becomes the primary account for managing Partner Central engagements and activities, including APN fee billing, solutions management, and APN Customer Engagement (ACE) opportunity tracking using the Partner Central APIs.

> **Important**
>
> This change is part of a larger migration to using AWS Identity and Access Management (IAM) to control user access to Partner Central. You must link to an AWS account that has the IAM roles and permissions needed to access Partner Central.

Account linking has other benefits:

- You can use **Partner Connections** to work on coselling deals with other partners. This can progress deals faster and expand your reach. For more information, see Partner connections in the *AWS Partner Central Sales Guide*.
- You can use the AWS Partner Central API to integrate Partner Central with your CRM system. Integration synchronizes engagements, opportunities, solutions, and real-time event notifications. For more information, refer to AWS Partner CRM integration in the *AWS Partner CRM Integration Guide*.
- If you're an ACE eligible partner who links to an AWS Marketplace seller account, AWS Demand Generation Representatives pre-qualify leads from AWS Marketplace and transfer validated AWS originated opportunities to you.

The following topics explain how to link accounts.

Topics

Prerequisites

The following topics list the prerequisites needed to link AWS Partner Central and AWS accounts. We recommend following the topics in the order listed.

> **Note**
>
> Due to user interface, feature, and performance issues, account linking does not support Firefox Extended Support Release (Firefox ESR). We recommend using the regular version of Firefox or one of the chrome browsers.

Topics

User roles and permissions

To link your AWS account with an AWS Partner Central account, you need people in the following roles:

Identity and Access Management (IAM) Administrator

Manages user permissions through IAM . Typically works in IT Security, Information Security, dedicated IAM teams, or Governance and Compliance organizations. Responsible for implementing IAM policies, configuring SSO solutions, handling compliance reviews, and maintaining role-based access control structures.

AWS Partner Central Alliance Lead or Cloud Administrator

Your company's primary account administrator. This person must have a business development or business leadership role and legal authority to accept AWS Partner Network terms and conditions. The Alliance Lead can delegate account linking to a Partner Central user with the Cloud Admin user role.

Selecting the right AWS account

Use the information in the following table to help decide which AWS account you should link with your Partner Central account.

Important

Consider the following when selecting an AWS account:

- AWS Partner Central requires an AWS account that uses IAM policies to control access.
- The linked AWS account manages APN fee payment, solutions, and APN Customer Engagement (ACE) opportunity tracking using the Partner Central APIs.
- AWS Partner Network features and APIs are available through the linked AWS account.
- AWS resources such as ACE opportunities, opportunity history, and multi-partner opportunity invitations are created in the linked AWS account and can't be transferred to other AWS accounts.
- The AWS account that you link to must be on a Paid AWS account plan. When you sign up for an AWS account, choose the Paid account plan. To upgrade an AWS account to the Paid AWS account plan, refer to Choosing an AWS Free Tier plan in the *AWS Billing User Guide*.
- AWS recommends linking an AWS account that is *not* used for the following purposes.
  - A management account, where you manage the account information and metadata for all of the AWS accounts in your organization.
  - A production account, where users and data interact with applications and services.
  - A developer or sandbox account, where developers write code.
  - A personal account where individuals for learn, experiment, and work on personal projects.
  - An AWS Marketplace buyer account, where you procure products from AWS Marketplace.

  Keeping the linked account separate from your AWS Partner Network engagements ensures flexibility for configurations specific to AWS Partner Central without affecting other environments. Doing so also simplifies financial tracking, tax reporting, and audits.

AWS Partner scenario	Example	AWS account options	Considerations
Scenario 1: You own AWS account(s) managed by a third-party and you are not registered as an AWS Marketplace seller	AWS Partners working with AWS Distributor partners	**Option 1:** Create an AWS account and link to it. **Option 2:** Link to an existing AWS account	**Option 1:** • Is it acceptable to bill the APN fee to this account? The AWS Managemen t account can pay the fee if the account is in an AWS Organization. • Is this where you want to access AWS Partner Network features and APIs? **Option 2:** • Same considera tions as Option 1 • Is this an AWS Managemen t, Production, Developer, or personal account? • Can you allow external personnel to access the account that manages AWS Partner Central engagements? • Is this account appropriate for

AWS Partner scenario	Example	AWS account options	Considerations
			managing Partner Central user access?
Scenario 2: You own AWS account(s) and are not registered as an AWS Marketplace seller	AWS Partners who don't transact through AWS Marketplace or partners in countries where AWS Marketplace is not available	Same as Scenario 1	Same as Scenario 1

AWS Partner scenario	Example	AWS account options	Considerations
Scenario 3: You own AWS account(s) and are registered as an AWS Marketplace seller with a single Marketplace seller account	AWS Partners who have a consolidated product listing in a single country or operate globally	**Option 1:** Create and link to a new AWS account **Option 2:** Link to an existing AWS account **Option 3:** Link to an AWS Marketplace seller account	**Option 1:** • Do you need access to AWS Marketplace features that require a linked Marketplace seller account? • Do you plan to join the AWS ISV Accelerate Program? See the program requirements. • Do you need to share AWS Partner Central and Marketplace resources like opportunities, offers, solutions, and product listings? • Would it be better to designate an AWS Marketplace seller account with the most product listings or transactions as a primary Marketplace seller account?

AWS Partner scenario	Example	AWS account options	Considerations
			• Is it acceptable to bill the APN fee to this account? **Option 2:** • Same considerations as Option 1 • Is this an AWS Management, Production, Developer, or personal account? • Is this account appropriate for managing Partner Central user access? **Option 3:** • Same considerations as Options 1 and 2 • Do you plan to create additional AWS Marketplace seller accounts? If so, is it acceptable to designate the current Marketplace seller account as a primary

AWS Partner scenario	Example	AWS account options	Considerations
			Marketplace seller account?
Scenario 4: You own AWS account(s) and are registered as an AWS Marketplace seller with multiple seller accounts	AWS Partners who have multiple product listings under different lines of business or have to meet regulator y and compliance requirements	Same as Scenario 3	Same as Scenario 3

Granting IAM permissions

The IAM policy listed in this section grants AWS Partner Central users limited access to a linked AWS account. The level of access depends on the IAM role assigned to the user. For more information about permission levels, refer to Understanding the role permissions later in this topic.

To create the policy, you must be an IT administrator responsible for an AWS environment. When finished, you must assign the policy to an IAM user or role.

The steps in this section explain how to use the IAM console to create the policy.

> **Note**
>
> If you're an alliance lead or cloud admin, and you already have an IAM user or role with AWS administrator permissions, skip to the section called “Linking accounts”.

To create the policy

1. Sign in to the IAM console.
2. Under **Access management**, choose **Policies**.
3. Choose **Create policy**, choose **JSON**, and add the following policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreatePartnerCentralRoles",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/PartnerCentralRoleForCloudAdmin*",
                "arn:aws:iam::*:role/PartnerCentralRoleForAce*",
                "arn:aws:iam::*:role/PartnerCentralRoleForAlliance*"
            ]
        },
        {
            "Sid": "AttachPolicyToPartnerCentralCloudAdminRole",
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/
PartnerCentralRoleForCloudAdmin*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::*:policy/
PartnerCentralAccountManagementUserRoleAssociation",
                        "arn:aws:iam::*:policy/AWSPartnerCentralFullAccess",
                        "arn:aws:iam::*:policy/
AWSMarketplaceSellerFullAccess"
                    ]
                }
            }
        },
        {
            "Sid": "AttachPolicyToPartnerCentralAceRole",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/PartnerCentralRoleForAce*",
```

```
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::*:policy/
AWSPartnerCentralOpportunityManagement",
                        "arn:aws:iam::*:policy/
AWSMarketplaceSellerOfferManagement"
                    ]
                }
            }
        },
        {
            "Sid": "AttachPolicyToPartnerCentralAllianceRole",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/PartnerCentralRoleForAlliance*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::*:policy/AWSPartnerCentralFullAccess",
                        "arn:aws:iam::*:policy/
AWSMarketplaceSellerFullAccess"
                    ]
                }
            }
        },
        {
            "Sid": "AssociatePartnerAccount",
            "Effect": "Allow",
            "Action": [
                "partnercentral-account-management:AssociatePartnerAccount"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SellerRegistration",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:StartChangeSet",
                "aws-marketplace:ListEntities",
```

```
                "aws-marketplace:DescribeEntity"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Choose **Next**.
5. Under **Policy details**, in the **Policy name** box, enter a name for the policy and an optional description.
6. Review the policy permissions, add tags as needed, and then choose **Create policy**.
7. Attach your IAM user or role to the policy. For information on attaching, refer to Adding IAM identity permissions (console) in the *IAM User Guide*.

Understanding the role permissions

After the IT administrator completes the steps in the previous section, alliance leads and others in AWS Partner Central can assign security policies and map user roles. The following table lists and describes the standard roles created during account linking, and the tasks available to each role.

Standard IAM role	AWS Partner Central managed policies used	Can do	Cannot do
Cloud admin	• PartnerCentralAccountManagementUserRoleAssociation • AWSPartnerCentralFullAccess: • AWSMarketplaceSellerFullAccess:	• Map and assign IAM roles to AWS Partner Central users. • Complete the same tasks as alliance and ACE teams.	
Alliance team	• AWSPartnerCentralFullAccess	• Full access to all seller operations on AWS Marketpla	Map or assign IAM roles to AWS Partner Central users. Only

Standard IAM role	AWS Partner Central managed policies used	Can do	Cannot do
	• AWSMarketplaceSellerFullAccess	ce, including the AWS Marketplace Management Portal. You can also manage the Amazon EC2 AMI used in AMI-based products. • Link AWS customer engagement opportunities with AWS Marketplace private offers. • Associate APN solutions with AWS Marketplace product listings. • Access the Partner Analytics dashboard.	alliance leads and cloud admins map or assign roles.

Standard IAM role	AWS Partner Central managed policies used	Can do	Cannot do
ACE team	• AWSMarketplaceSellerOfferManagement • AWSPartnerCentralOpportunityManagement	• Create AWS Marketplace private offers. • Link AWS customer engagement opportunities with AWS Marketplace private offers.	• Map or assign IAM roles to AWS Partner Central users. Only alliance leads and cloud admins can map or assign roles. • Use all the AWS Marketplace tools and features. • Use the Partners Analytics dashboard.

Creating a permission set for single sign-on

The following steps explain how to use the IAM Identity Center to create a permission set that enables single sign-on for accessing AWS Partner Central.

For more information about permission sets, refer to Create a permission set in the *AWS IAM Identity Center User Guide*.

1. Sign in to the IAM Identity Center console.
2. Under **Multi-account permissions**, choose **Permission sets**.
3. Choose **Create permission set**.
4. On the **Select permission set type** page, under **Permission set type**, choose **Custom permission set**, then choose **Next**.
5. Do the following:

   A. On the **Specify policies and permission boundary** page, choose the types of IAM policies that you want to apply to the permission set.

By default, you can add any combination of up to 10 AWS managed policies and customer managed policies to your permission set. IAM sets this quota. To raise it, request an increase to the IAM quota **Managed policies attached to an IAM role** in the Service Quotas console in each AWS account where you want to assign the permission set.

B. Expand **Inline policy** to add custom JSON-formatted policy text. Inline policies don't correspond to existing IAM resources. To create an inline policy, enter custom policy language in the provided form. IAM Identity Center adds the policy to the IAM resources that it creates in your member accounts. For more information, see Inline policies.

C. Copy and paste the JSON policy from AWS Partner Central and AWS Account Linking pre-requisite

6. On the **Specify permission set details** page, do the following:

A. Under **Permission set name**, type a name to identify this permission set in IAM Identity Center. The name that you specify for this permission set appears in the AWS access portal as an available role. Users sign into the AWS access portal, choose an AWS account, and then choose the role.

B. (Optional) You can also type a description. The description appears in the IAM Identity Center console only, not the AWS access portal.

C. (Optional) Specify the value for **Session duration**. This value determines the length of time that a user can be logged on before the console logs them out of their session. For more information, see Set session duration for AWS accounts.

D. (Optional) Specify the value for **Relay state**. This value is used in the federation process to redirect users within the account. For more information, refer to Set relay state for quick access to the AWS Management Console.

> **Note**
>
> You must use an AWS Management Console URL for the relay state. For example: `https://console.aws.amazon.com/ec2/`

E. Expand **Tags (optional)**, choose **Add tag**, and then specify values for **Key** and **Value (optional)**.

For information about tags, refer to Tagging AWS IAM Identity Center resources.

F. Choose **Next**.

7. On the **Review and create** page, review the selections that you made, and then choose **Create**.

   By default, when you create a permission set, the permission set isn't provisioned (used in any AWS accounts). To provision a permission set in an AWS account, you must assign IAM Identity Center access to users and groups in the account, and then apply the permission set to those users and groups. For more information, refer to Assign user access to AWS accounts in the *AWS IAM Identity Center User Guide*.

Linking AWS Partner Central and AWS accounts

The following steps explain how to use AWS Partner Central to link your accounts. You must be an alliance lead or cloud admin to complete these steps. Also, the IAM permissions policy listed earlier in this guide controls the linking and role mapping tasks you and other AWS Partner Central users can perform. For more information about those tasks, refer to Granting IAM permissions.

For more information about account linking, refer to the Account Linking User Guide in Partner Central.

> **Note**
>
> - AWS Partner Central uses the term *AWS Marketplace Account Linking*, but all partners can link accounts, including partners without AWS Marketplace accounts.
> - Partners in Amazon Web Services India Private Limited (AWS India) can link without registering a business name.

1. Sign in to AWS Partner Central as an alliance lead or cloud admin.

   > **Note**
   >
   > If your organization uses single sign-on (SSO), use those credentials to sign in to your AWS account first, then sign in to AWS Partner Central.

2. In the **AWS Marketplace** section of the AWS Partner Central home page, choose **Link Account**.
3. On the **AWS Marketplace Account linking** page, choose **Link Account**.
4. On the AWS account sign-in page, choose **IAM user**.

5. Enter the ID of the AWS account and sign in.

> **Note**
>
> - If you need account information, contact the administrator who completed the prerequisites listed above.
> - SSO users automatically skip to the next step.

6. Navigate through the self-service linking experience:

A. Review the AWS account ID and the associated AWS Marketplace seller profile legal name and choose **Next**.

> **Note**
>
> If your AWS account is not registered as a seller, provide your legal business name to be registered on AWS Marketplace.
> Partners in Amazon Web Services India Private Limited (AWS India) can link without registering a business name. Proceed by choosing **Next**.

B. Review the IAM roles and the managed policies attached to them, then choose **Next**.

C. (Optional) To bulk map the IAM roles to the partner users with Alliance team and ACE partner roles, select the checkbox under each role section.

A partner user cannot access AWS Marketplace features, such as linking private offers to ACE opportunities, without an IAM role mapped to their partner user account. If you choose not to bulk assign, you must manually map an IAM role to a partner user after linking the accounts.

D. Review the information, then choose **Submit**.

You are directed to AWS Partner Central with your account successfully linked and the default IAM roles created in your account.

7. (Optional) To use custom policies that enable access to AWS Marketplace features within AWS Partner Central, refer to the next topic, Using custom policies to map users.

Using custom policies to map users

The topics in this section explain how to map AWS Partner Central users to AWS IAM roles. Mapping enables single sign-on access for users across AWS Partner Central and AWS. plus other features such as product and offer linking.

Topics

Role mapping prerequisites

Before mapping, you must complete the following prerequistites:

- Create IAM roles in the AWS account. For more ionformation, refer to Create a role using custom trust policies in the *AWS Identity and Access Management User Guide*.
- To allow AWS Partner Central to map AWS IAM roles, add the following custom trust policy to the roles.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "partnercentral-account-management.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- For AWS Partner Central users with the ACE user role, grant permissions to perform the `ListEntities` and `SearchAgreements` actions. For more information, refer to Controlling access to AWS Marketplace Management Portal in the *AWS Marketplace Seller Guide*.
- Link your AWS Partner Central account to an AWS Marketplace account.

To map IAM roles to your AWS Partner Central users, you must create IAM roles with the permissions you want to provide to your users. For cloud admin users, you can only map the cloud admin IAM role created in your account during the account linking process.

You can create one or more IAM roles to associate with your AWS Partner Central users. The role names must start with **`PartnerCentralRoleFor`**. You can't choose a role unless the name begins with that text.

You can attach custom or managed policies to the IAM role. You can attach the AWS Marketplace managed policies such as `AWSMarketplaceSellerFullAccess` to the IAM roles and provide access to your AWS Partner Central users. For more information about creating roles, refer to Creating an IAM role (console) in the *IAM User Guide*.

Connecting ACE opportunities with AWS Marketplace private offers

To enable ACE users to attach AWS Marketplace private offers to ACE opportunities, map them to an AWS IAM role in AWS Partner Central.

Prerequisites

Complete the following before mapping users to AWS Marketplace IAM roles:

- When you link an AWS Marketplace account to AWS Partner Central, provide `AWSMarketplaceSellerFullAccess` or, minimally, `ListEntities/SearchAgreements` to the IAM role assigned to ACE users. This is required to enable ACE users to attach AWS Marketplace private offers to ACE opportunities.
- (Optional) To grant minimal permission, add a customer managed policy to your AWS account and to the IAM role you create for ACE managers and users. Refer to the following policy as an example:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:SearchAgreements",
                "aws-marketplace:DescribeAgreement",
                "aws-marketplace:GetAgreementTerms",
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:StartChangeSet"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws-marketplace:PartyType": "Proposer"
                },
                "ForAllValues:StringEquals": {
                    "aws-marketplace:AgreementType": [
                        "PurchaseAgreement"
                    ]
                }
            }
        }
    ]
}
```

Mapping users to AWS IAM roles

Use the procedures in this section to map and unmap AWS Partner Central users to AWS IAM roles.

To map an AWS Partner Central user to an AWS IAM role

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **Account linking** section of the AWS Partner Central homepage, choose **Manage linked account**.
3. In the **Non-cloud admin users** section of the **Account Linking** page, choose a user.
4. Choose **Map to IAM role**.
5. Choose an IAM role from the dropdown list.
6. Choose **Map role**.

To ummap an AWS Partner Central user from an AWS IAM role.

1. Sign in to AWS Partner Central as a user with the alliance lead or cloud admin role.
2. In the **Account linking** section of the AWS Partner Central homepage, choose **Manage linked account**.
3. In the **Non-cloud admin users** section of the **Account Linking** page, choose the user you want to unmap.
4. Choose **Unmap role**.

Unlinking AWS Partner Central and AWS accounts

When you link AWS Partner Central to an AWS account, AWS resources, such as APN Customer Engagement (ACE) opportunities, are created in the linked AWS account. If you unlink to that AWS account and then link to a different AWS account, you lose access to the AWS resources in the original account.

The following list describes what happens to your AWS resources when you unlink from an original account and link to a different account. Consider the impact on your business before you submit an unlinking request.

AWS Partner Central users lose the ability to perform tasks listed in Understanding the role permissions. You must reassign the applicable IAM permissions after linking the new AWS account.

For example, ACE users can't link ACE opportunities with private offers until IAM permissions in the new AWS account have been reassigned.

You lose access to pending multi-partner opportunity invitations, and partners must re-invite you to them.

For example, say AnyCompany has five unique invitations from AWS partners to collaborate on multi-partner opportunities. If AnyCompany unlinks from the original AWS account and links to a different account without accepting the invitations, all five partners must re-invite AnyCompany in order to collaborate on multi-partner deals.

You lose access to shared multi-partner opportunities, and partners must re-share them even if you're the primary ACE opportunity owner.

For example, say AnyCompany uses Partner Connections to share an ACE opportunity with Example Corp. If AnyCompany unlinks from the original account and links to a different account, the ACE opportunity still exists, but AnyCompany can't access it, even as a primary owner, until Example Corp shares the opportunity again.

The APIs stop sending updates to ACE opportunities. For this reason, AWS recommends completing your sales engagements prior to unlinking.

For example, say AnyCompany uses the Partner Central APIs to integrate their CRM systems with AWS Partner Central, and AnyCompany uses their CRM system to manage those ACE opportunities. If AnyCompany unlinks from the original account and links to a different account, any AWS updates to the ACE opportunities by will not sync and partners won't be notified about the updates.

You can't access or edit linked private offers associated with ACE opportunities.

For example, say AnyCompany linked AWS Partner Central with an AWS Marketplace seller account, and then associated the ACE opportunities with private offers. If AnyCompany unlinks from the original account and links to a different account, AnyCompany can't access linked ACE opportunities and private offers. In addition, the linked private offers can't be associated with ACE opportunities from the newly linked AWS account.

The system automatically rejects AWS Originated (AO) opportunities pending acceptance. AWS Sales teams see the AO's as rejected and share them again with the partner.

For example, if AnyCompany unlinks from the original account and connects to a different account, AnyCompany can't accept or reject pending AO's, which expire automatically in five days. The AWS Sales team sees the rejected AO's and has to share them again.

If you decide to link to a different AWS account, AWS recommends:

- Accepting or rejecting pending AWS originated opportunities.
- Accepting or rejecting pending multi-partner opportunity invitations.
- For ACE opportunities linking to or disconnecting from private offers as needed.
- Completing sales engagements prior to unlinking if possible.

> **Note**
>
> There is no impact if you relink to the original AWS account.

To request unlinking

1. Sign in to AWS Partner Central as an alliance lead or cloud administrator.
2. Under **Account linking**, choose **Manage linked account**.
3. Choose **Unlink account**.
4. Review the warning message and select a reason for unlinking your account.
5. Enter **`confirm`** and choose **Open support case**.
6. On the confirmation banner, choose **View case details** to track the progress of your request.

Account linking FAQ

The following topics answer frequently asked questions about linking AWS Partner Central accounts with other AWS accounts.

Who can link AWS Partner Central and AWS accounts?

Alliance Leads and Cloud Admins can link accounts, but only after an IAM administrator completes the prerequisites.

Alliance Leads can delegate linking by assigning Cloud Admin roles to existing users. For more information, refer to Managing user roles and assignments later in this guide.

Is there any technical effort required, and what should I plan for?

Identify an IAM administrator with console access to your target AWS account. The IAM administrator must complete the prerequisites before you initiate linking.

Who is my IAM administrator?

IAM administrators typically work in IT security, information security, or dedicated IAM teams. They implement policies, configure SSO, handle compliance reviews, and maintain access controls.

Why do we need to have a Paid account to link AWS Partner Central and AWS accounts?

Starting November 15, 2025, you must have a Paid account plan to renew your APN membership. On that date, AWS begins processing APN fee billings only for Partner Central accounts with linked AWS accounts at renewal. For more information, refer to APN Fee Requirement Change for 2025. Marketplace sellers also need paid accounts for service usage.

Can I unlink and re-link a new account, if I do not want to use my existing linked account as my primary account?

You can unlink an AWS account, but doing so creates data persistence issues and requires manual reconciliation efforts. For more information about unlinking AWS accounts, refer to Unlinking AWS Partner Central and AWS accounts earlier in this guide.

I don't have an AWS account that I can use for APN engagement. How do I create one?

Coordinate with your IAM administrator to identify the team responsible for account approval and provisioning. For instructions on setting up an AWS account, refer to Create an AWS account in the *AWS Account Management Reference Guide*. Be sure to select the Paid account plan.

How do I provision a new AWS account?

Your IAM administrator should know the team responsible for account approval and provisioning. For information about setting up a new AWS account, refer to Create an AWS account in the *AWS Account Management Reference Guide*. During that process, be sure to select the **Paid account plan**. For more information about account plans, refer to Choosing an AWS Free Tier plan in the *AWS Billing User Guide*.

Which IAM policies should I use?

You use AWS managed policies for the account linking prerequisites. By default, account linking uses AWS managed policies to assign IAM roles during account linking. However, IT admins can use custom AWS Marketplace policies to assign IAM roles to AWS Partner Central users such as an ACE team. The roles enable users to link ACE opportunities with AWS Marketplace private offers. For more information, refer to Using custom policies to map users later in this guide.

The links in the following list take you to the *AWS Managed Policy Reference*.

AWS managed policies

- AWSPartnerCentralFullAccess: – Provides full access to AWS Partner Central; features and related AWS services.
- AWSPartnerCentralOpportunityManagement: – Provides necessary access for opportunity management activities.
- AWSMarketplaceSellerOfferManagement: – Enables seller access to offer and agreement management activities.

For more information about the AWS Partner Central managed policies, refer to AWS managed policies for AWS Partner Central users later in this guide.

For more information about the AWS Marketplace managed policy, refer to AWS managed policies for AWS Marketplace sellers in the *AWS Marketplace Seller Guide*.

Custom AWS Marketplace policies

- `aws-marketplace:ListEntities` and `aws-marketplace:SearchAgreements` – Enables users to link ACE opportunities and AWS Marketplace private offers.
- `aws-marketplace:GetSellerDashboard:` – Grants access to the AWS Partner Central & Marketplace dashboard.

For more information about the custom AWS Marketplace policies, refer to Policies and permissions for AWS Marketplace sellers in the *AWS Marketplace Seller Guide*.

Why can't I complete account linking? I have alliance lead privileges

You must have the alliance lead or cloud admin *role*, not the privileges.

How do I unlink accounts?

Follow the steps in Unlinking AWS Partner Central and AWS accounts earlier in this guide.

What happens to linked ACE opportunities + MPPO if I unlink an account?

If you unlink and re-link to a different AWS Marketplace seller or AWS account, linked objects disappear. If a partner re-links to the same AWS Marketplace seller or AWS account, linked objects remain.

How can I manage partner user access to a linked account?

Alliance leads use AWS Partner Central User Management to assign IAM roles to AWS Partner Central users and grant them access to a linked account. They can also remove the mapped roles to remove access a linked account.

In addition, each standard IAM role created during account linking comes with limited permissions. For more information about them, refer to Understanding the role permissions earlier in this guide.

Selecting the PartnerCentralAceRole checkbox created 3 roles. Why?

You use that option to bulk assign IAM roles to the Alliance, Cloud Admin, and ACE teams. The linking process creates the roles. Partners can use the IAM console to delete unwanted roles.

For more information, refer to Updated Account Linking User Guide in AWS Partner Central.

Why can't we register our legal business name during account linking?

Ensure you submitted an accurate account name. The AWS ID you select may already be in use, and it cannot be shared by multiple parties, especially if your company is merging. For guidance on what to during a merger, refer to:

- AWS Partners M&A Policy and FAQs
- How do I merge AWS Partner Central accounts?

Why do I get the “Missing IAM Role Mapping”, “Missing Permission”, “Access denied”, and “Your AWS Marketplace IAM role does not have the required permissions” errors?

The messages appear for the following reasons:

- An AWS Partner Central user wasn't mapped to an IAM role. Ask the alliance lead or cloud admin to map the appropriate role to the user. For more information, refer to the AWS Partner Central & AWS account linking guide.
- AWS Partner Central users with mapped IAM roles need to update their existing policies. For more information about the latest prerequisites, refer to Prerequisites earlier in this guide.

Can I associate AWS Marketplace private offers and Channel Partner private offers with ACE opportunities?

Yes, but you must link accounts first. You use AWS Partner Central to associate AWS Marketplace private offers with ACE opportunities. You use **Partner Connections** to associate Channel Partner private offers with ACE opportunities. Both methods require account linking before you can use them. For more information, refer to Partner Connections in the *AWS Partner Central Sales Guide*.

Getting support

Ask questions to Amazon Q

Amazon Q (Q) is an AI-powered assistant that provides real-time, personalized support to through natural language to search across Partner Central and Marketplace knowledge sources and return concise summaries and recommendations. Support is available by selecting the Q logo and launching the chat window in the console, selecting Ask Amazon Q in the top search bar, or Diagnose with Q when an error is returned on widgets, features, and pages throughout the console.

If Amazon Q does not respond with the information you need, you can create a case with support by selecting Partner Central Support from left navigation menu.

Support

In AWS Partner Central, in the left-side navigation panel you will see three options for getting support: Partner Central support, Marketplace support, and Marketplace refund support. If you are unable to log into your account, you can file a ticket to the APN Support team here.

For support for any AWS Partner Network related queries, choose Partner Central support. This will re-direct to the legacy Partner Central experience, where users can submit a ticket directly to the APN Support team. See details below.

For support on AWS Marketplace listings and other Marketplace-related queries, choose Marketplace support. This will re-direct to the AWS Marketplace Management Portal page where users can submit a ticket directly to the Marketplace support team.

For support specifically on refund related to AWS Marketplace listings, choose Marketplace refund support.

> **Note**
>
> The AWS Console includes a support option in the upper right-hand corner of the global navigation. However, this directs users to the general AWS Support channel. For the fastest response to APN, Partner Central, or Marketplace inquiries, this support channel is not recommended.

Partner Central support

AWS Partner Support is a case-management feature for partners to engage with APN Support. On the Partner Support page, you can open a new case, review your open and previous cases, and read articles related to common issues, questions, and concerns posed by other users. You can track correspondence on open cases, respond directly from AWS Partner Central, and upload files to help you communicate your issues with AWS Partner support.

AWS Partner Support gives you the ability to enter details about your issue so that the support team can help you more efficiently.

- **Type of Case** – Choose the type of support case you want to open. This helps to route your request to the right team.
- **Question Type** – Choose the option that best aligns with the type of question you want to ask the support team.
- **Get Specific** – Choose a more specific question type.
- **Subject** – Enter a descriptive subject for your support ticket.
- **Description** – Describe your issue in detail.
- **Attachments** – Add any attachments to help describe your issue.

If you are locked out of AWS Partner Central, you can get support by doing the following:

1. Navigate to the AWS Partner Team contact page of the AWS Partner Network Knowledge Base.
2. Complete the contact form and choose **Submit**.

Document history for the AWS Partner Central Getting Started Guide

The following table describes the documentation releases for AWS Partner Central Documentation.

Change	Description	Date
AWS Partner Central Agents launch	Launched AWS Partner Central agents, new AI-powered capabilities designed to accelerate partner co-selling with AWS.	March 16, 2026
Updated managed policies	Updated the managed policies `AWSPartnerCentralFullAccess`, `AWSPartnerCentralSandboxFullAccess`, `AWSPartnerCentralOpportunityManagement`, and `PartnerCentralIncentiveBenefitManagement` to add Partner Central Agents session management capability through the Model Context Protocol. For information, see AWS Partner Central updates to AWS managed policies.	March 13, 2026
Updated existing user management documentation	Updated User management documentation with added instructions for AWS IAM role-based access implementation for AWS partner central.	March 6, 2026

Updated existing managed policies	Updated AWSPartnerCentralOpportunityManagement, AWSPartnerCentralChannelManagement, and AWSPartnerCentralMarketingManagement managed policies with Amazon Q permissions to support Partner Assistant chatbot functionality.	February 23, 2026
Updated existing managed policies	Updated AWSPartnerCentralFullAccess managed policy with Amazon Q permissions and AWS Marketplace Agreements read permissions.	February 11, 2026
Added new managed policy	Added the `PartnerCentralIncentiveBenefitManagement` managed policy. For more information, see PartnerCentralIncentiveBenefitManagement.	February 11, 2026
Added new managed policies and updates to existing	Added the `AWSPartnerCentralMarketingManagement` managed policy. For more information, see AWSPartnerCentralMarketingManagement. Updates to: AWSPartnerCentralFullAccess, AWSPartnerCentralOpportunityManagement, AWSPartnerCentralChannelManagement.	November 30, 2025

AWS Partner Central console launch	Launched AWS Partner Central in the AWS Management Console with comprehensive new features and migration from legacy system. Added new documentation topics including console navigation, funding, dashboard customization, account management, partner analytics, funding programs, solution creation, CRM integration, and migration guidance. Updated existing documentation for console-based workflows and IAM integration. Key new features include: Console navigation, funding benefts, dashboard, partner analytics, migration tools, Controlling access in AWS Partner Central, and enhanced account management.	November 30, 2025

Added new managed policies and updates to existing	Added the `AWSPartnerCentralChannelManagement` and `AWSPartnerCentralChannelHandshakeApprovalManagement` managed policies. For more information, see AWSPartnerCentralChannelManagement, AWSPartnerCentralChannelHandshakeApprovalManagement. Updates to: AWSPartnerCentralFullAccess.	November 19, 2025
Added documentation for Channel Management	Channel management enables partners to qualify for channel program benefits when transacting with end customers using Billing Transfer.	November 19, 2025
Updates to Partner Assistant documentation	Moved information that was formerly in the AWS Partner Central FAQ to AWS Partner Assistant and added a nested FAQ page specific to that product.	March 17, 2025
Added account unlinking instructions	Instructions were added in Unlinking your AWS Partner Central account from an AWS Marketplace account.	January 15, 2025

Added new managed policy and updates to existing	Added the `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` managed policy. For more information, see AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy. Updates to: AWSPartnerCentralFullAccess, AWSPartnerCentralOpportunityManagement, AWSPartnerCentralSandboxFullAccess.	December 4, 2024
New AWS Partner Assistant	AWS Partner Assistant is a generative AI-powered chatbot for AWS Partners. It is accessible from both Partner Central and AWS Marketplace Portal (AMMP).	November 25, 2024
Added new managed policy	Added the `AWSPartnerCentralFullAccess` AWS managed policy. For more information, see AWS managed policy: `AWSPartnerCentralFullAccess`.	November 18, 2024
Added managed policy	Added the `AWSPartnerCentralOpportunityManagement` AWS managed policy. For more information, see AWS managed policy: `AWSPartnerCentralOpportunityManagement`.	November 14, 2024

Added managed policy	Added the `AWSPartnerCentralSandboxFullAccess` AWS managed policy. For more information, see AWS managed policy: `AWSPartnerCentralSandboxFullAccess`.	November 14, 2024
Clarification	Updated linking accounts prerequisites for clarity.	June 5, 2024
First release	First release of the AWS Partner Central Getting Started Guide.	November 10, 2023