Azure Partner Admin Link

Method Overview and Frequently Asked Questions

Contents

Method Overview

As a partner you help the customer to design, build, deploy or manage a solution on Azure. Currently, outside of the Cloud Solution Provider (CSP) program, partners who do consulting or provide managed services on Microsoft Azure, do not have tools to track and report on the impact they are driving across all customer engagements.

Microsoft is creating a new method to help you better track your engagements with Azure customers. This will be based on your access to customer's Azure resources. With this new method, you can link the user credentials or application credentials you have been granted within a customer's Azure environment to your Microsoft Partner Network ID.

How does this method work?

Today as a partner, you use following methods to get access for customer's Azure resources:

- **Guest user:** The customer adds with guest users from partner organization using Azure AD business-to-business (B2B) collaboration capabilities and assign the role to the Azure resources. Please see [Add guest users from another directory](#) for information.

- **Directory account:** The customer can create a new user from partner organization in their own directory and assign the role to the Azure resources.

- **Service Principal:** The partner develops an application; the customer registers the application to their directory and give access to Azure resources with service principals.

Once you have access to customer resources, you can use PowerShell or CLI to link your Microsoft Partner Network ID (MPN ID) to the user id or the application service principal.

What is the benefit of linking the Partner ID to user or service principal credentials?

Microsoft will provide partners with an end to end view of their customer engagements for all users who have added the MPN ID to their credentials. You will receive a high-level view on the status and health of the resources you have under management within customer accounts. Both Microsoft and the partner can also use this information to drive closer engagement between partners and the Microsoft sales teams and a more consistent view of a **partner's impact on Azure growth.**

Who can link the partner ID?

The user from partner organization who has been granted access rights within a customer environment can attach a partner ID to the credentials within each the customer environment that they have been granted access.

Once a partner ID has been assigned can it be changed? Is there a limit to the number of changes possible?

Yes, partner ID assignment can be changed, added, removed as many times as the partner wishes.

What if an individual or application has credentials in multiple customer environments?

The link between the MPN ID and the credentials is done per customer tenant. You can associate and MPN ID to the user in each customer environment.

What is the difference between Partner Admin Link and Azure Partner Customer Usage Attribution?

The key clarification is that PAL associates a partner with credentials and Customer Usage Attribution associates the partner with an application. It is not the customer's subscription or tenant that gets tagged. This is important because there is only one customer, but there can be many sets of credentials or applications. It is important to mention that Digital Partner of Record (DPOR) does remain the only method for partners to receive financial incentives at this time, however, if PAL and CUA work as well as we expect, we will start to shift that direction.
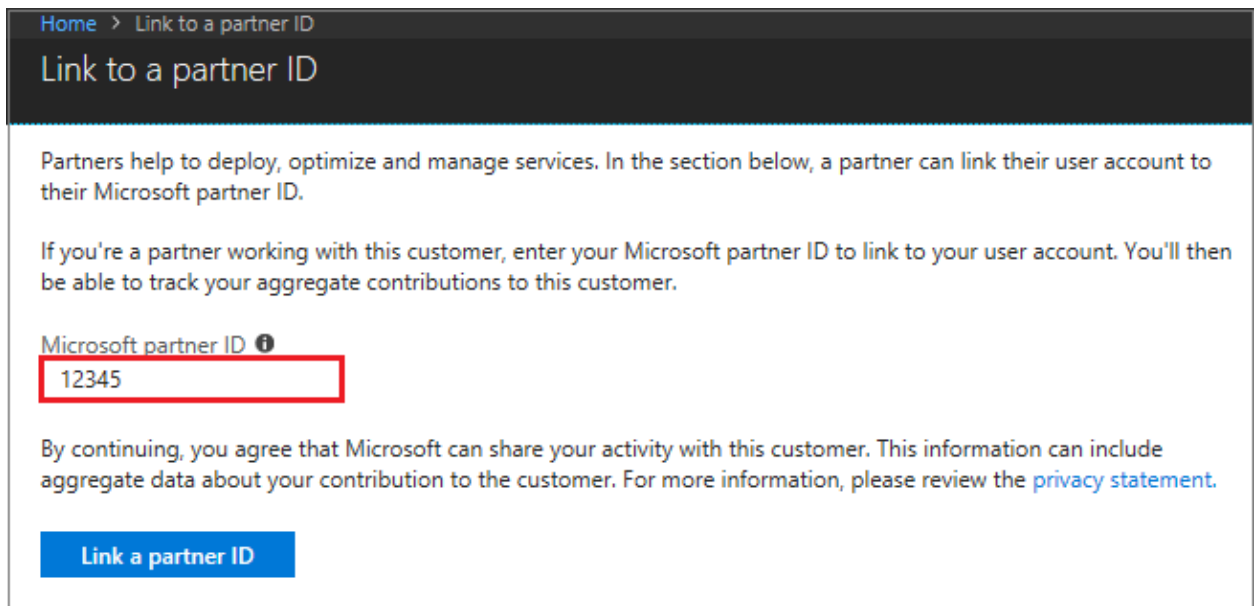
[Back to top](#)

# Instructions to link your Partner ID

Azure Management Portal

The simplest way to associate an MPN ID with admin credentials is within the Azure Management Portal.

1. Go to link to a partner ID in the Azure portal.

2. Sign in to the Azure portal.

3. Enter the Microsoft partner ID. The partner ID is the Microsoft Partner Network (MPN) ID of your organization.

4. To link partner ID for another customer, use the directory switcher. Under Switch directory, choose your directory.
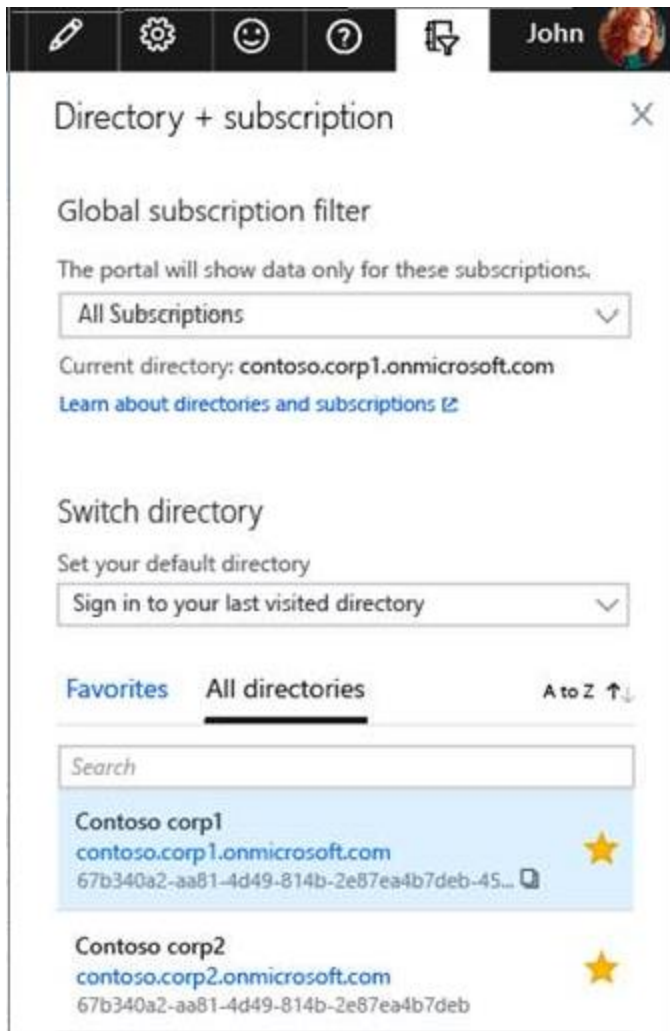
PowerShell

1. Use either PowerShell Console or PowerShell Integrated Scripting Environment (ISE). Ensure that AzureRM and AzureAD modules are installed.

2. Install AzurePartnerRP module using following instructions:

   - Open "Windows PowerShell" in admin mode.

   - Set the execution policy

     Set-ExecutionPolicy Unrestricted -Force

   - Install the latest version of PowerShellGet. Make sure that PowerShellGet version is greater than 1.6.0.

     Install-Module -Name PowerShellGet -Repository PSGallery -Force

   - Install the module

Install-Module -Name AzureRM.ManagementPartner -AllowPrerelease

3. Login to your customer's AD Tenant either with user id or service principal , using the instructions from [Log in with Azure PowerShell](#).

   User

   Login-AzureRmAccount -TenantId <Tenant ID>

   ```
   PS C:\WINDOWS\system32> Login-AzureRMAccount -tenantID 72f988bf-86f1-41af-91ab-2d7cd011db47

   Account         : dhiraj_gandhi@hotmail.com
   SubscriptionName :
   SubscriptionId   :
   TenantId         : 72f988bf-86f1-41af-91ab-2d7cd011db47
   Environment      : AzureCloud
   ```

   Application/Service Principal

   $cred = Get-Credential -UserName $svcprincipal.ApplicationId -Message "Enter Password"

   Login-AzureRmAccount -Credential $cred -ServicePrincipal -TenantId <Tenant ID>

   ```
   PS C:\WINDOWS\system32> $cred = Get-Credential -UserName $svcprincipal.ApplicationId -Message "Enter Password"
   PS C:\WINDOWS\system32> Login-AzureRmAccount -ServicePrincipal -Credential $cred -TenantID 04081b9f-c8b4-424b-86b9-ce44721c2b23

   Account         : 73495fe0-8b1c-4c1e-b951-711c766f5483
   SubscriptionName :
   SubscriptionId   :
   TenantId         : 04081b9f-c8b4-424b-86b9-ce44721c2b23
   Environment      : AzureCloud
   ```

4. Link the Partner ID

   new-AzureRmManagementPartner -PartnerId <MPN ID>

   ```
   PS C:\WINDOWS\system32> new-AzureRmManagementPartner -PartnerId 5127255

   PartnerId TenantId                              ObjectId                              State
   --------- --------                              --------                              -----
   5127255   72f988bf-86f1-41af-91ab-2d7cd011db47  67a9be6b-3998-4c2e-9ebf-2c1438dc9bff Active
   ```

   - *A valid MPN ID will be required. If the MPN ID provided is not valid you will see an error.*

5. Get the linked Partner ID:

   - *allows you to verify the MPN ID that was linked to the credentials*

   get-AzureRmManagementPartner

   ```
   PS C:\WINDOWS\system32> get-AzureRMManagementPartner

   PartnerId TenantId                              ObjectId                              State
   --------- --------                              --------                              -----
   5127255   72f988bf-86f1-41af-91ab-2d7cd011db47  67a9be6b-3998-4c2e-9ebf-2c1438dc9bff Active
   ```

6. Update the linked Partner ID

        Update-AzureRmManagementPartner -PartnerId <MPN ID>

```
PS C:\WINDOWS\system32> Update-AzureRmManagementPartner -PartnerID 212312

PartnerId TenantId                             ObjectId                             State
--------- --------                             --------                             -----
212312    72f988bf-86f1-41af-91ab-2d7cd011db47 67a9be6b-3998-4c2e-9ebf-2c1438dc9bff Active
```

7. Delete the linked Partner ID

        remove-AzureRmManagementPartner -PartnerId <MPN ID>

```
PS C:\WINDOWS\system32> remove-AzureRmManagementPartner -PartnerID 212312
```

Command Line Interface (CLI)

1. Install Azure CLI 2.0 using following instructions.

   https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest

   You can also use Azure Cloud Shell.

2. Install the Azure Management Partner CLI Extension.

   ```
   az extension add --name managementpartner
   ```

3. Login to customer's tenant either with user id or service principal, using the following instruction.

   ```
   az login --tenant <tenant>
   ```

4. Link the new Partner ID for this user.

   ```
   az managementpartner create --partner-id <MPN ID>
   ```

5. Get the linked Partner ID

   ```
   az managementpartner show
   ```

6. Update the linked Partner ID

```
az managementpartner update --partner-id <MPN ID>
```

7. Delete the linked Partner ID

```
az managementpartner delete --partner-id <MPN ID>
```

Frequently Asked Questions (FAQ)

Additional Guidance on linking MPN IDs

If I have multiple people with credentials in a customer's environment do all users need to link their MPN ID to their credentials?

Partners should associate their MPN ID to each set of credentials within a customer's environment.

Can multiple partners be set at the resource level?

An unlimited number of partners can show up because PAL associates the partner with the credentials in use. Whether they are influencing a subscription, resource group, or resource instance is defined by the scope and level of admin permissions. Many customers set up a unique subscription for each application or partner; however, there are other ways to ringfence resources within a single subscription (resource groups), so we do expect that partners often overlap. Another use case like this would be one partner doing migrations or deployments and another delivering support.

Which roles can associate their MPN ID to a customer's environment? Do they have to be a Global Administrator in the direction?

Any Azure admin role will be able to add PAL. We support all RBAC roles at any permission level or scope. The assumption is that admin access – even read only – to a customer's environment demonstrates trust and influence.

If a consultant is using their work credentials as a "guest" in multiple customer accounts will they need to associate the MPN ID once or multiple times?

If a consultant from the partner is using the same credentials in multiple customer's environments, they will need to associate an MPN ID in each customer environment. The association happens on a per customer environment basis and is not inherited in all customer environments.

Is every Guest User/Directory account of the partner required to do PAL or is a single user sufficient?

We suggest using PAL on as many accounts as possible if they have different permission levels or scopes so that you receive the full credit possible. This also helps mitigate the risk that one account is removed or consultant changes projects.

We have multiple MPN IDs which should we use?

You should choose the MPN ID that you would like to receive credit for the customer engagement. If you have multiple MPN IDs for credit in other programs you may want to follow a similar approach for this program.

What happens if there are multiple partners having different workloads in the same customer subscription?

Multiple partners can appear in the same tenant, subscription, resource group, or even resource instance.

Will another partner be able to write over my MPN ID if I link it within a customer account?

No, the link is established as an attribute for a set of user credentials. Only the individual who is using the credentials can set or change the MPN ID.

If some partners go for manual set up of Partner Admin Link and other partners use a GUID or API, which is the overriding process, assuming both are set at the same level – either Tenant, subscription, or resource?

The association with the partner's MPN ID is done on the credentials or application. There is no override or conflict between multiple partners unless they are sharing the same username and password.

Is PAL set up at Tenant level, Subscription level or Resource?

PAL can be as granular as Resource Instance (ie. single VM); however, technically, it's set on the user account and the scope of ACR measurement is whatever admin permissions that user account has within the environment. Admin scope can be subscription, resource group, or resource instance using standard Azure admin roles. For example, if you are an SI and I am a company, I might hire you to do a project. I can give you an admin account in order to deploy, configure, and support an application, and I can scope your access to a Resource Group. If you use PAL and associate your MPN ID with that admin account, Microsoft will measure the consumed revenue from the services within that resource group.

Do we need to follow the instructions to link our Partner ID listed above in the Azure portal AND the PowerShell AND the Command Line Interface – or are all three options and we choose only one method?

Azure portal, PowerShell, and Command Line are all options and do not need to be used together. PowerShell is ideal for scripting and bulk updates, whereas the portal is better for people who prefer to have a visual UI experience.

CSP

Does PAL apply only on Enterprise Agreements (EAs) and Pay-as-you-go or will it work on CSP workloads as well? What about indirect CSP?

PAL is intended to measure influence of partners outside the CSP channel when they are doing work within a customer's subscription. If the partners is selling Azure through CSP, PAL is not necessary – and thus not enabled – for the CSP admin agents group because the telemetry and association is already established.

Can the CSP Reseller be set as PAL as it is different from the actual CSP Indirect partner.

It is technically possible but would not provide any new information.

If a CSP Direct sells Azure, but customer engages an SI for project services and IP/Solution on top of this Azure, can the SI be set a PAL?

Yes, this is one of the important scenarios to support.

If an ISV drives a SaaS application on a subscription purchased from a CSP Reseller today the consumption counts automatically to the CSP Reseller, not the ISV. Can the ISV be recognized for competency consumption using PAL on a CSP subscription?

Yes, this is one of the important scenarios that we want to enable.

What is the difference between PAL and Delegated Admin Privilege (DAP), which is part of CSP?

DAP is related to having permissions within a customer's environment, whereas PAL is to associate a partner's MPN ID with the account that has admin permissions.

Reporting

When will reporting be available?

Reports are available to partners within the Microsoft Partner Network (MyInsights dashboard) and Partner Center (Analyze tab).

- Partner Center Dashboard
- MyInsights Dashboard

What is included in the reporting?

Microsoft will be able to link the credentials used within the customer's environment with the RBAC role and scope of access assigned by the customer. We will be able to associate the usage of the individual Azure resources that the credentials have access to.

What is the cadence of the reporting updates?

They are updated after fiscal month close, which is about the 10th of each month for the prior month (includes time to process the data). For expectation setting, I always plan to find the newest information on the 14th of the month.

Does the customer receive reporting as well?

Customers already have tools to track and manage administrative access to their environment. Customers will receive an additional report when a partner has added their MPN ID to their credentials.

Digital Partner of Record (DPOR)

Is Partner Admin Link (PAL) similar to the Digital Partner of Record (DPOR)?

Linking a partner's administration credentials to an MPN ID is a completely new mechanism to connect a partner's management activities to customer usage. It allows for a more direct connection to the Azure resources that a partner is managing. It is based on the customer granting administration rights to the partner and does not require the customer to do any additional tagging on behalf of the partner. This new method also tracks the link between a partner and customer usage at a much more granular level.

Does it make sense for me to advise my Azure Delivery teams to pursue both DPOR and PAL for a given customer?

Yes. If you've already used PAL, you'll be well situated for any new benefits in the future.

Is DPOR the only way to receive financial incentives based on a Customer's Azure consumption numbers?

DPOR is the primary way for services. CSP is the hero reseller motion that also allows a single bill for managed services.

If within the same customer subscription, one partner is DPOR (i.e. LSP) and other multiple partners (SIs, ISVs, etc.) get set as PAL for specific resources they work with, will Microsoft double count the impact (not for incentives)? For example, in the ACR report or towards MPN Competencies ACR requirement?

The incentives and competency teams are still defining business logic, so this will be documented clearly in the future and may change between now and then. However, at this point, yes we will count the partner's influence even when they are overlapping with another partner. For example, one partner

may develop a solution and another partner support the infrastructure behind it, and we want to recognize that both are playing an important role in the customer's success.

What happens when a customer decides as an internal policy to not set any partner as DPOR, due to incentive tied to it?

For Partner Admin Link (services) and Customer Usage Attribution (development), customers do not need to take any action and associating their MPN ID with the credentials or application is the responsibility of the partner.

Incentives

What are the financial and other incentives for attaching with Partner Admin Link?

Partner Admin Link will have a financial incentive soon, and it will also count towards the Cloud Platform competency. Currently, DPOR is the method for both.

What are the specific credit/incentive types that accrue to a partner from Azure PAL?

Currently, it is Cloud Platform competency (goes live soon but accrual has started already). We are very interested in creating financial incentives also.

Will Azure usage be tied to any monetary incentive programs for partners?

Soon. DPOR is and will continue to be the partner incentive program.

Can I use influenced Azure revenue derived through the partner admin link to qualify for partner competencies?

Not currently.

Customer actions and privacy

Linking a partner's "administration" credentials to an MPN ID is essentially the PAL mechanism to connect a partner's management activities to customer usage. It allows for a more direct connection to the Azure resources that a partner is managing. It is based <u>on the customer granting administration rights to the partner</u> and does not require the customer to do any additional tagging on behalf of the partner. This new method also tracks the link between a partner and customer usage at a much more granular level.

Does the customer have to do anything?

The customer will not have to do any unique work to support the linking of the MPN ID to the partners administration credentials. Customers will be responsible for granting the partner access to their environment, but customers should only grant credentials to only those required to conduct management operations over the customers Azure resources and applications running on those resources.

Does this feature grant the partner any administrative rights or access to data?

No, the customer grants access and partners will only have administrative access or the ability to see data that has been granted by the customer. Where the partner is unable to view usage data reporting will be aggregated and anonymized.

Should I request administrative access from my customers to show up in reporting?

You should only request access when the engagement with your customer requires administrative access to their environment. Customers should carefully control who has administrative rights to their infrastructure and applications. Customers should not receive pressure to provide administrative access if they do not deem it necessary.

What happens if the customer changes the scope of access or revokes administration access to their Azure environment?

The link is tied to the administrative credentials within the customer's environment. If the customer changes the scope of access, or if the admin account or admin permissions are removed, the partner-customer association is ended. Partner Admin Link is designed to track influence on revenue during services delivery.

How should I describe this to my customer?

This new capability does not impact a partner's scope of access. It does not give the partner access to any service, data or insight that was not explicitly granted by the customer. The customer will receive reporting on partners who have linked the credentials to their MPN ID that will augment their existing identity tracking.

Resources

For partners:

1. Overview Webcast: Get Recognized for Driving Azure Consumption (Sept 2018)

2. For management and consulting services with admin access
   a. Azure Partner Admin Link Documentation
   b. Contact: AzurePartnerAdmin@microsoft.com

3. For solutions deployed in customer environments
    a. [Azure Customer Usage Attribution Documentation](#)
    b. Contact: AzureISVPilot@microsoft.com

4. Existing method used for partner incentive programs
    a. [Digital Partner of Record](#)
    b. [Cloud Solution Provider](#)

5. Reporting and Insights
    a. [Partner Center Dashboard](#)
    b. [MyInsights Dashboard](#)