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 this method works?**

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

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

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

- **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 the Azure Portal UI, 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.

**Instructions to link your Partner ID**

**Azure Portal UI –**

2. Login to the customer’s tenant with your credentials
3. Use the following link to add an MPN ID: https://ms.portal.azure.com/#blade/Microsoft_Azure_Billing/managementpartnerblade

*Navigation through Portal Settings coming soon*

**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>

Application/Service Principal

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

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

4. Link the Partner ID

new-AzureRmManagementPartner -PartnerId <MPN ID>

```
PS C:\WINDOWS\system32> new-AzureRmManagementPartner -PartnerId 5127255
PartnerId          TenantId          ObjectId          State
----------------- --------------- --------------- ------
5127255           72F9888bF-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`

   ![Command Output]

   PartnerId TenantId ObjectId State
   --------- -------- --------- -----
   5127255 72f988bf-86f1-41af-91ab-c7d011db47 67a9be6b-3998-4c2e-9ebf-2c1438dc9b6f Active

6. Update the linked Partner ID

   `Update-AzureRmManagementPartner -PartnerId <MPN ID>`

   ![Command Output]

   PartnerId TenantId ObjectId State
   --------- -------- --------- -----
   212312 72f988bf-86f1-41af-91ab-c7d011db47 67a9be6b-3998-4c2e-9ebf-2c1438dc9b6f Active

7. Delete the linked Partner ID

   `remove-AzureRmManagementPartner -PartnerId <MPN ID>`

   ![Command Output]

   CLI -

1. Install Azure CLI 2.0 using following instructions.

   You can also use [Azure Cloud Shell](https://aka.ms/AzureCloudShell).

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>
Additional Q&A

When will reporting be available?

A beta version of reporting will be available to partners beginning in May 2018. The beta reporting will be a high level, aggregated view while final compliance policies are defined and implemented.

What will be 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.

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.

Is this 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.

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

Not at this time. Digital Partner Of Record (DPOR) remains the partner incentive program.

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

Not at this time.

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 administrative access to their Azure environment?**

The link is tied to the administrative credentials within the customers environment. If the customer changes the scope of access the ID link will reflect the changes in the will reflect or revokes administrative access.

**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.

**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.

**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.

**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.

**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.

*disclaimer: this documentation is part of a preview program. Microsoft reserves the right to change the product at any time during the preview.*