FAQ: Recognising Customer ACR Influence with PAL and CUA

Disclaimer

This FAQ has been provided by the UK OCP team to help partners understand and work with the new recognition mechanisms, Partner Admin Link (PAL) and Customer Usage Attribution (CUA).

The document is provided under NDA and the intent is to help partners get recognition against the Azure Consumed Revenue (ACR) they have influence so that their true impact is visible. It is a working document and will be updated as the understanding grows.

The document may also change location over time, so please always use either of the following short URLs to access the most recent version:

- aka.ms/palfaq
- aka.ms/cuafaq

If you find anything within the document to be incorrect then please contact either richard.cheney@microsoft.com and/or david.gristwood@microsoft.com.

Summary

A number of options exist to help partners get recognition for the **Azure Consumed Revenue** (ACR) that they drive or influence in customer subscriptions.

This document explores the different mechanisms available to recognise ACR, discusses the applicability of each and provides some guidance on how to best engage with partners, based on experiences in the field with partners.

In particular, this document covers:

- Cloud Solution Provider (CSP)
- Digital Partner of Record (DPoR)
- Partner Account Link (PAL)
- Customer Usage Attribution (CUA, a.k.a. Template Tracking or GUID Tracking)

Which of these should you be looking at?

- For an Independent Software Vendor (ISV) selling their IP into customers subscription, then **Customer Usage Attribution** (GUIDs) is usually the right option
- **Partner Admin Link** is designed more for managed service providers (MSPs)
- **Digital Partner of Record** is an older mechanism that has largely been superseded by CUA and PAL

Why is ACR recognition important?

The two key metrics used to track Azure progress are Azure Consumed Revenue (ACR) and Azure Customer Adds (ACA). ACR growth is vital for a partners visibility within Microsoft. A partner, especially one that may be influencing a lot of ACR, but it is all materialising in the customer subscription, and therefore is unrecognised influence, is understating their impact and can "fly under the radar" in terms of recognition and reward.

Some of these mechanisms also drive partner rebates, or are required to track incentives within certain partner programmes.

There are several mechanisms that are available, but under the covers they all eventually tie Azure telemetry against a partner's Microsoft Partner Network (MPN) ID.

For general information for both recognition and incentives then make use of these resources:

- Overview Webcast: Get Recognized for Driving Azure Consumption (Sept 2018)
- Incentive Overview and Guides

Cloud Solution Providers

How do you track ACR with Cloud Solution Providers?

Automatically! One of attractions of Cloud Solution Providers (CSP) is that CSP resellers are instantly recognised for the ACR in those CSP subscriptions. They are right in the middle of the transaction and contractual process and they usually manage the subscriptions on behalf of the end customer.

The same is true of the two step CSP Indirect process, where both the CSP Indirect Provider and CSP Indirect Reseller are recognised for their influence.

Digital Partner of Record

What about Digital Partner of Record?

Digital Partner of Record (DPoR) is a mechanism to link an partner's MPN ID to a customer subscription. It is usually used on Enterprise Agreement (EA) or Direct (pay as you go. or PAYG) subscriptions.

DPoR has been around for some time and is well known.

What problems are there with DPoR?

DPoR has a couple of major limitations:

1. **DPoR only allows one partner to be recorded per subscription** DPoR's 1:1 link is far too coarse and simplistic for today's complex partner channel. We have a mix of licence providers (LSPs), service integrators (Sis), managed service providers (MSPs) and independent software vendors (ISVs), all working with customers and the solutions they are running on Azure. (Even these lines are blurring and many partners don't fit neatly into just one of those descriptions.) Partners get involved at different points in time and may influence a subset of the resources in a subscription. Some organisations are very organised at assigning DPoR to themselves for a new subscription, but they may not be the partner organisation with the most influence in that subscription. There is a difficult and manual process to get multiple partners recognised for DPoR, but that is a workaround rather than a solution.

2. **The customer assigns DPoR to the partner** There is zero incentive for a customer to do this retrospectively, and many are inherently suspicious of these processes. Therefore it often doesn't happen unless it is done as part of a standard process at the beginning, such as the subscription creation, or project initiation.

These are some of the core reasons why Partner Admin Link and Customer Usage Attribution were created.

Will DPoR disappear?

Probably, in time. Once the new mechanisms take hold then DPoR is likely to become obsolete and then removed.

It is possible that it will remain and be used to reflect the influence that some advisory partners have, but that would still be a difficult assignment process.

Also DPoR does provide a rebate, so it will be painful to remove it before any incentives relating to PAL and CUA are worked out.

Partner Admin Link

What is Partner Admin Link?

Partner Admin Link (PAL) is designed for managed service providers (MSPs). Assuming the MSP has access to resources in the customer subscription then they can link their those accounts to their MPN ID. From that point onwards the telemetry for those resources (and only those resources) will be linked to the partner.

There is an overview webinar for PAL:

> Get Recognized for Driving Azure Consumption on-demand link (Feb 2019)

How do those partners access and manage customer resources?

There are three ways that they can authenticate into the customer subscription and manage resources on their behalf:

1. Azure Active Directory Business to Business (AAD B2B)

   The admins use their normal AAD identities (belonging to the partner's tenancy), which have been assigned an RBAC role in the customer's subscription

2. Service Principal

   A service principal is created and assigned an RBAC role in the customer subscription, and all partner admins use those credentials to gain access

3. "Guest" IDs

   The customer creates users within their own tenancy and gives those credentials to the partner for the partner admins to use

The first is the preferred option, particularly if it uses a security group that is used as that is very manageable as people join and leave. Service principals are often used by configuration management software such as Terraform, Chef, Puppet, Ansible etc. but you do lose the audit trail against the individual partner admins.

Note that Contributor role is usually assigned at the subscription level, but more limited inbuilt roles (such as VM Contributor, Network Contributor) are also used, or fine tuned custom roles. The scope of partner management may be further reduced by assigning those roles to specific resource groups (or resources) rather than at the subscription level.

OK, so how do they link the resources?

There are steps to link an ID to the partner's MPN ID, and it is a quick and easy process using either the portal, CLI or PowerShell. The instructions are at aka.ms/partneradminlink, and it is a really simple process. Just make sure you have authenticated into the customer tenancy and subscription correctly first.

It is a good idea for every partner ID to be linked to the MPN using PAL. This will ensure the telemetry remains attached to the MPN, even in the event of an employee leaving the partner. (If only one person links to the MPN then this would be plausible.)

At a technical level it is possible to configure PAL without any interaction with the end customer, but Microsoft has an ethical stance on transparency and so the customer should be informed as a courtesy.

My partner does not have access to the customer's subscription. Can they still use PAL?

No, you need to have access to the customers resource to use PAL to link to the MPN ID.

(Partner Admin Link does not address all of the scenarios where DPoR has historically been assigned.)

My partner has access, but only has Reader or Billing Reader role. Is that sufficient for PAL?

Partners need to have a level of admin rights within the customer tenant.

Are there any other exceptions that prevent the PAL association?

Yes. Here are some of the common reasons:

- Admin role from legacy ASM model rather than ARM's RBAC model
- Credentials are member of CSP Admin Agents group
- Customer subscription is sponsored or internal Microsoft
- User does not authenticate into customer tenant before setting PAL
- Resources within account scope have not generated any consumption revenue

The exception for the CSP Admin Agents security group prevents double counting of CSP and PAL in the same subscription.

Can multiple partners use PAL within the same customer subscription?

Yes, it does allow for more complex scenarios. It is cleaner if the RBAC assignments do not overlap, i.e. one partner has access to the resource they manage (and no more), and the other partner has access to only their managed resources.

How do I check if PAL is working correctly?

Microsoft employees should be able to see the results in https://ocpinsights.microsoft.com. Search for your partner and then select Microsoft Azure in the Cloud Product Performance section in the left pane. Filter Partner Attach Type to Partner Admin Link.

How does where partners can check on their own PAL recognition?

There are a couple of places you can go to:

1. Partner Center Dashboard
2. MyInsights Dashboard

Customer Usage Attribution

Note: Customer Usage Attribution is also known as Tracked Templates or GUID Tracking.

What's Customer Usage Attribution and who uses that?

Customer Usage Attribution (CUA) is designed to help recognise the ACR influenced from ISVs. It is sometimes referred to as "Tracked Templates". If you hear GUIDs being tracked, then it is CUA.

The mission statement for CUA is "Measure the holistic impact our Partners have on our Azure business REGARDLESS of how the solution is deployed."

The idea comes from the ACR tracking already in use for solutions deployed from the Azure Marketplace and AppSource marketplaces, and extends that idea to ISV solutions deployed via other channels.

ISVs are automatically recognised for the ACR they influence when solutions are deployed directly from those marketplaces.

The problem is that many of the AppSource listings are "Contact Me" solutions rather than deployed from the marketplace. The solutions are then deployed as part of a consultative engagement, and we have had no way of easily linking those resources back to the ISV and their solution. Sometimes the consultative engagement is done by another partner, making use of the ISV partner's IP, and again we lose track of it all.

Customer Usage Attribution provides a new mechanism to track these and reflect the ISV partner's true influence, regardless of the channel that their solution is deployed through.

There is an excellent public facing document that covers CUA - https://aka.ms/customerusageattribution- and this should be the first port of call for anyone to fully understand how CUA works.

Where do these GUIDs come from?

First step is for the ISV to generate a GUID, which is a unique 128 bit number, for each solution and/or channel. The GUID is then attached to the deployment so that those **newly** deployed resources are then linked to the GUID and therefore the ISV partner.

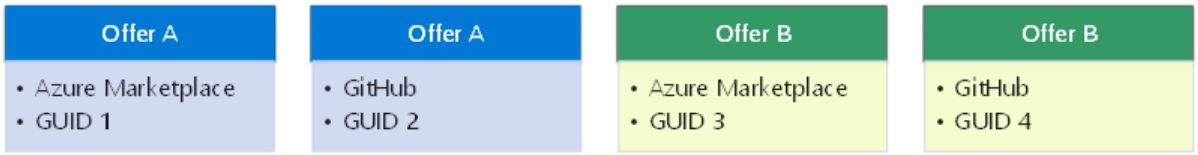
GUIDs are generated manually by the ISV, and they have to be registered, as defined in the public documentation. This is an important step - the system will not record telemetry against an unregistered GUID.

In the future the registration screen will generate the GUIDs automatically.

Is it best to create a GUID per customer deployment?

No, a GUID should not be created for each customer.

One GUID per solution per channel is the recommendation. For example, take a GUID that represents the solution deployed following a end customer opportunity via the Contact Me button in AppSource. You would will see those in the reporting, and you would also be able to filter separately by end customer name or individual subscriptions.



Some partners have had push back when they start registering large number of GUIDs, as the system isn't designed for this type of use. So keep it as simple as is sensible, otherwise there is an unnecessary admin headache. And think about what reporting the partner needs and will find the most useful.

How do the ISVs then use those GUIDs?

The GUID can be attached in one of three ways:

1. ARM Templates

   Add a pid-<GUID> resource within the master template. All other resources will be linked to that GUID using the correlationId.

2. Terraform Provider

   Set the optional partner_id argument (in the azurerm provider) to the GUID, and store in module etc.

3. Append the user agent header

   For everything else, you can append pid-<GUID> to the userAgent header for the REST calls. Works for the SDKs, direct REST API calls, Ansible etc.

For more detail, look at aka.ms/customerusageattribution.

From a transparency perspective then an ISV's customers should be made aware that the telemetry is being collected. Some of the ISVs that have adopted early have updated their EULA to this effect.

Does it help to have a slick DevOps process?

Yes! The piloting of CUA with partners has highlighted that many have not yet adopted modern, slick DevOps best practises around CI/CD, and as a result, adding the GUID to a deployment has had to be done manually, which introduces the scope for mistakes or for it to be missed out entirely.

This situation is even worse for partners who sell through partners, such as Systems Integrators, who deploy the software as part of a bigger business transformation engagement. These partners have to edit or write their own deployment scripts, and as they have no incentives or rewards around GUIDs, it often get left out. Automated deployment is key to ensuring the GUIDs gets deployed and the partner gets the ACR recognition.

How does the partner report on CUA?

This has proved one of the biggest issues with CUA to date. Partners can register a GUID in the cloud portal, deploy the resource, but have no way of accessing reports themselves. During the early days, it required someone inside Microsoft, with access to the Azure Health Report, to manually check. Although there is a ACR spreadsheet that can be used for this process, it is slow and cumbersome. So we developed some Power BI reports optimised for GUID tracking that queried the health data directly, and they have proved very useful.

Partner Center will be the place for partners to report on ACR, and at the time of writing, March 2019, this is starting to be deployed to partners, and so any partner that is doing CUA should ensure they get early access to Partner Center.

Can I attach a GUID to something already deployed?

No, you can't. It only gets attached at the time the resources are created. This is the most common request from partners, but technically there is no easy way to do this.

And that GUID has to be registered in advance. If you deploy something without a registered GUID then it won't be attached and registering it later won't magically attach it. Register those GUIDs in advance.

Storage is a classic example. If the ISV's solution creates lots of nice big ACR hungry storage blobs into an existing storage account then you won't see the GUID against that telemetry data. The storage account needs to be created by the solution's automation with that pre-registered GUID.

With storage there is the option to create a second storage account with a GUID attached to it, and then use AZCOPY utility to copy contents between the two, then delete the original. Compute based deployments tend to be more complex and often the best option is to wait until there is a major update that requires a new deployment, and hook into that.

Miscellaneous

Recognition of partner influenced ACR is good. But what about partner incentives?

At the moment the only ACR tracking mechanisms that have associated partner incentives are CSP and DPoR. There is no incentive attached to PAL or CUA.

The intention is to introduce incentives attached to that telemetry, but this is being worked through at the moment and there are no timelines or firm commitments.

There has been some discussion on whether any new incentive could and should be backdated. There is already good reason to use PAL and CUA as soon as possible to start lighting up those dashboards, but if they do backdate any incentives then your partners should use PAL or CUA to attach themselves to that telemetry data as soon as possible.

I have an ISV solution which is deployed and then managed by a service integrator. How does that work?

That should work fine. The ISV would use CUA in their ARM or Terraform configuration files. And then once the solution has been deployed by the SI then the partner should have access via the managed services. Use Partner Admin Link as normal.

For those ISVs that always partner other organisations for ongoing service management, then there is another construct that may come into play - Managed Applications. These combine a set of templates and a UI definitions for a service catalogue entry, plus an AAD authorisation into the customer subscription for the deployed resources.

The ARM templates could include a GUID registered by the ISV. And the Managed Application definition would permit the managed service partner access to the resources. At which point they could use PAL to link their MPN.