

By [Scott Sugar](#) on February 04, 2021

Power BI Usage Metrics Across All Workspaces: Step by Step

[Insights & Automation](#)

In this blog, I want to talk about [Power BI](#) Usage Metrics across all Workspaces.

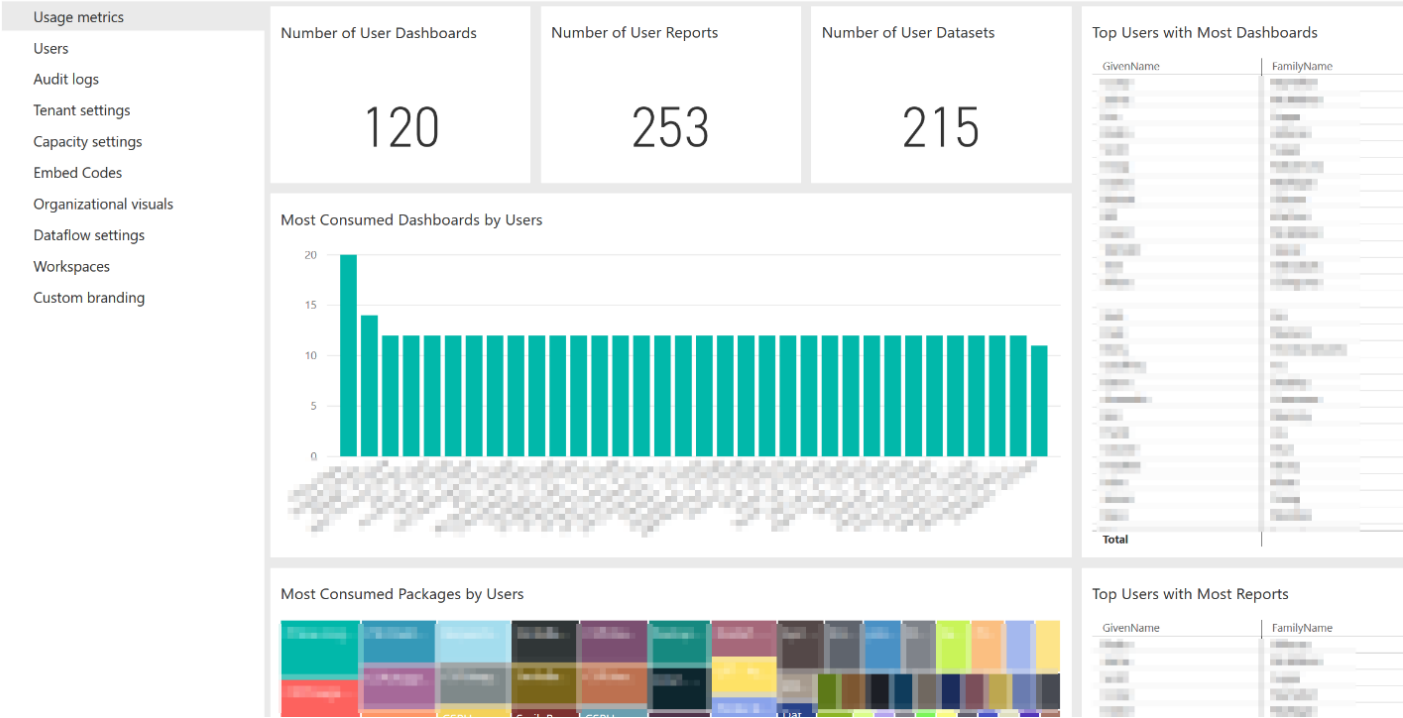
You've heard the adage, "You can't manage what you can't measure". So, when it comes to managing your tenant's online Power BI service, how do you measure the usage of your reports, dashboards, and datasets? Which reports are getting the most attention? By whom? Are there unused reports or workspaces that could be cleaned up?

There are Usage Metrics at the report/dashboard level that can be saved, edited, and unfiltered to show usage across an entire workspace, but for organizations with more than a few workspaces, monitoring usage at the workspace level is not scalable and doesn't allow for a unified view of usage across the tenant.

The online Power BI service does offer Usage Metrics in the Admin portal, but it's not customizable or interactive, and seems to be more focused on "who has how many reports/dashboards" rather than the question I set out to answer "who's using the service, and what are they looking at?"

So, let's look at Power BI Built-In Usage Metrics in the Admin portal:

Admin portal



Power BI Usage Metrics: Solution Walkthrough

Set up Pre-Requisites

We have a few things we need to set up in order to get this solution working:

Azure AD Global Admin account

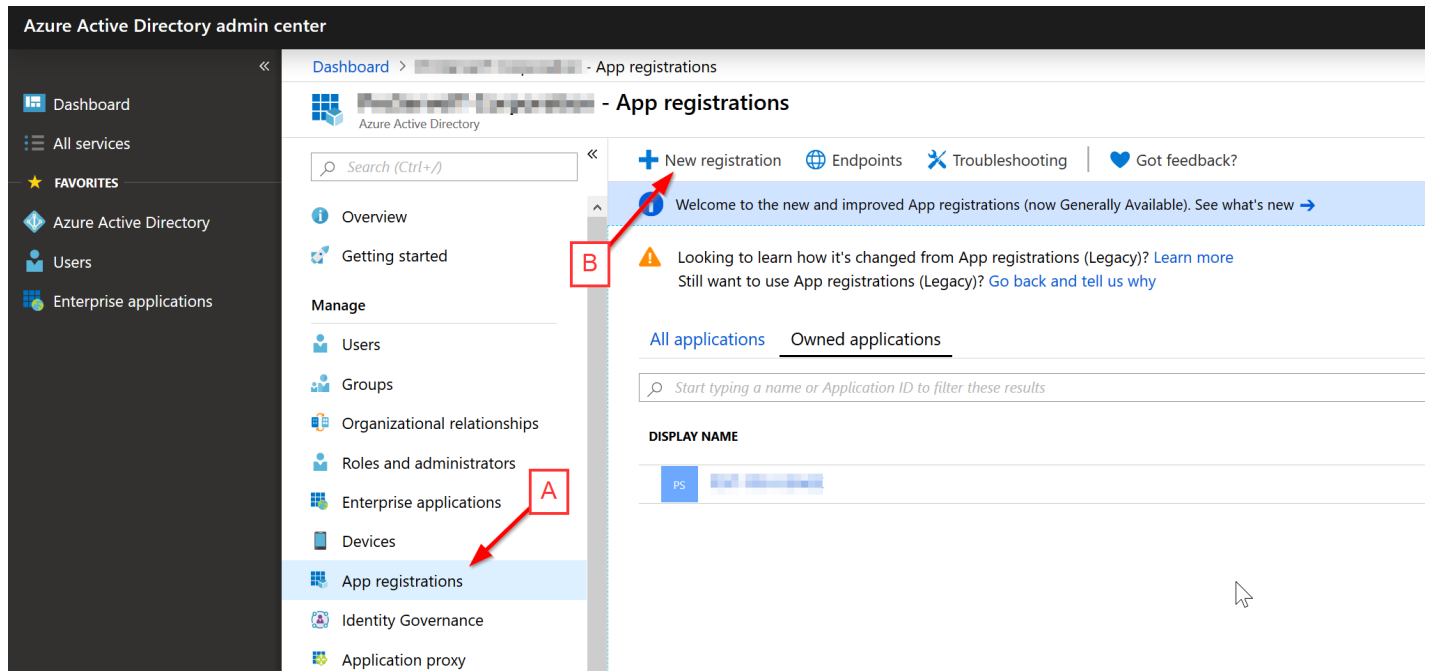
Azure AD Application - to help us authenticate to the O365 Management APIs

Power BI Streaming Dataset - to hold the Power BI activity logs

Create an Azure AD Application

1. Login to Azure AD Admin Portal and Create a new Azure AD Application

- . Click App Registrations
- . Click New Registration



2. Register Azure AD Application

- . Enter Application Name
- . Select Supported Account Types (default is fine if just gather activity logs for one tenant)
- . Click Register

Azure Active Directory admin center

Dashboard > App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Blog-PBI-Usage ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼ e.g. https://myapp.com/auth

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

3. Add API Permissions

- . Click API Permissions
- . Click "Add a permission"
- . Click "Office 365 Management APIs"

Azure Active Directory admin center

Dashboard > App registrations > Blog-PBI-Usage > API permissions

Blog-PBI-Usage - API permissions

API permissions

Applications are authorized to call APIs when they are granted permissions by all the permissions the application needs.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also be able to permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Users will not be shown a consent screen when using the application.

Grant admin consent for ProServeIT Corporation

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Dynamics ERP
Programmatic access to Dynamics ERP data

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

4. Request API Permissions

- Click "Application Permissions"
- Select ActivityFeed.Read
- Select ServiceHealth.Read
- Click "Add permissions"

Request API permissions

< All APIs

Office 365 Management APIs
https://manage.office.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<div>B</div> ActivityFeed (1)	
<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization	Yes
<input type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	Yes
ActivityReports	
<div>C</div> ServiceHealth (1)	
<input checked="" type="checkbox"/> ServiceHealth.Read Read service health information for your organization	Yes
ThreatIntelligence	

D

Add permissionsDiscard

4a. Grant Admin Consent for your org

. Click "Grant admin consent for ..."