Outpost24

Vulnerability Management made easy

A Guide to Setup EWP Workload Analytics for Azure

Version: 1.0
2018-Nov-23

Table of Contents

1 PRE-REQUISITES 4

2 CREATE APPLICATION ON AZURE ACCOUNT 5

2.1 ADD A NEW APPLICATION 5

2.2 GRANT PERMISSIONS 8

3 EWP CONFIGURATION 10

4 ANNEX 11

About This Document

This document provides users with an overview on how to set up EWP Workload Analytics for Azure.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

→

1 Pre-requisites

1. Log-in to Azure with an account that has administration permissions on Azure Active Directory.
2. Select the right active directory folder that contains the subscriptions you want to scan.
3. To register an Azure account on EWP, you need to create two applications on the account:
    - To perform the auto-discovery of assets on Azure.
    - To perform automatic CIS checks such as hardening Azure foundation benchmark.

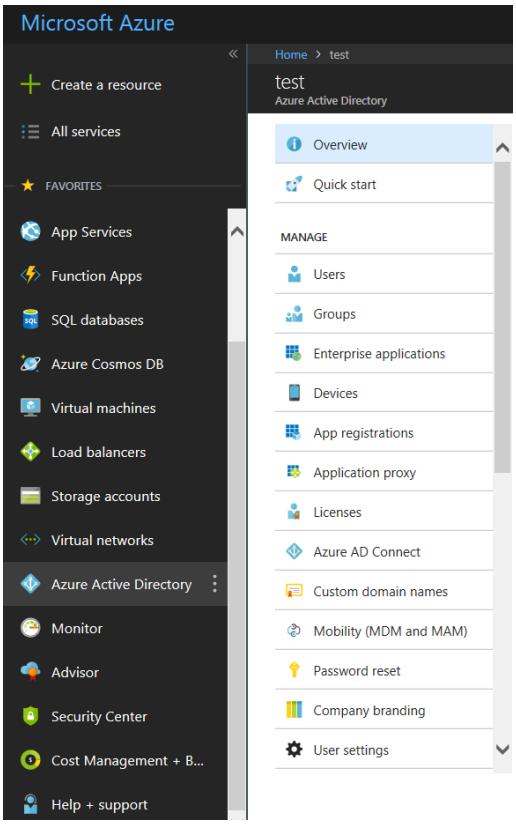
***Note**: You can use the same application for both auto-discovery of assets on Azure, and the hardening assessment of Azure as both are read-only access.*

2 Create Application on Azure Account

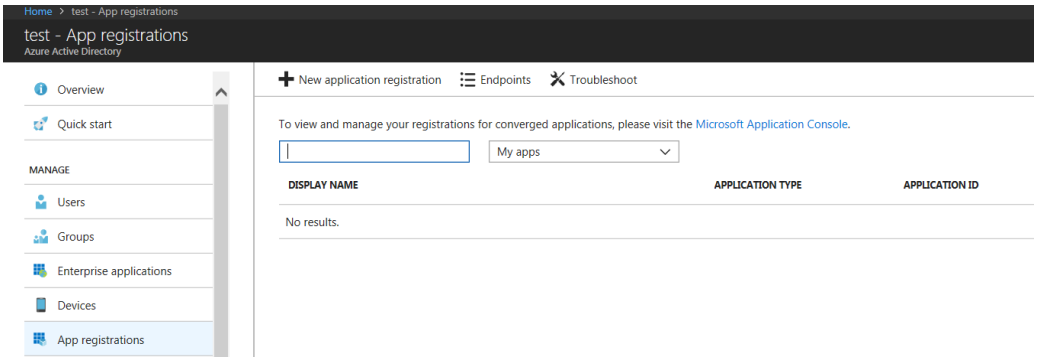
Follow the below instructions to create an application on Azure account for EWP Client ID.

2.1 Add a New Application

1. Click on **Azure Active Directory** on the left panel.

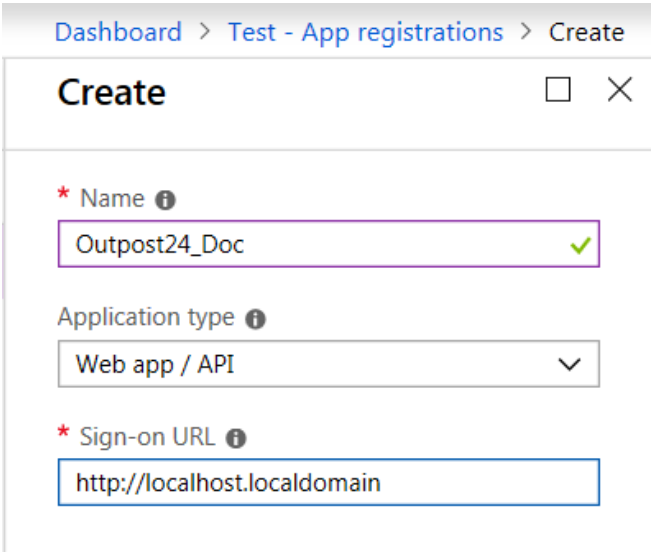


2. Click on **App registrations**.

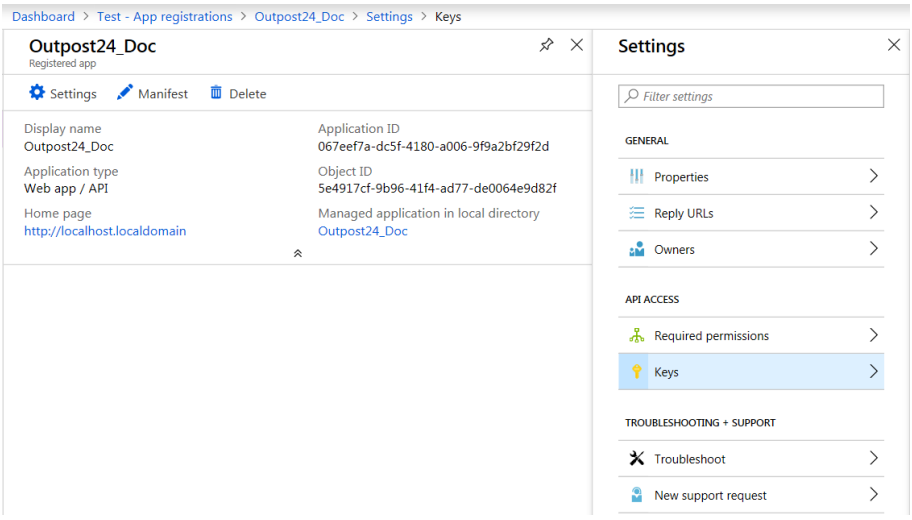


3. Click on **+ New application registration**.

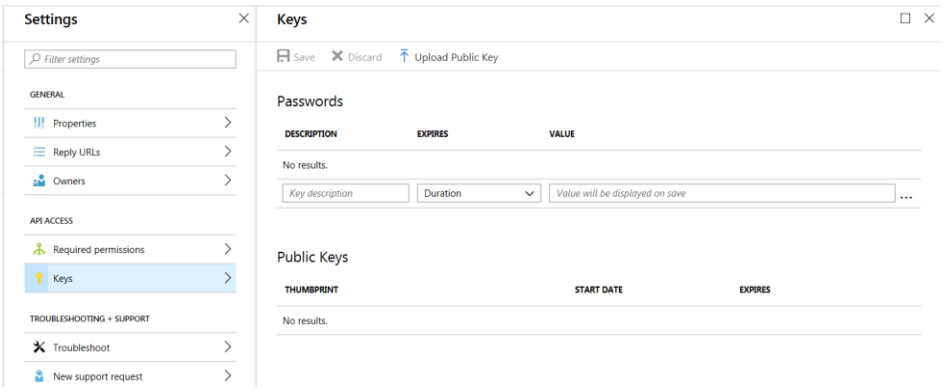
4. Create a new Application of type **Web App / API**.



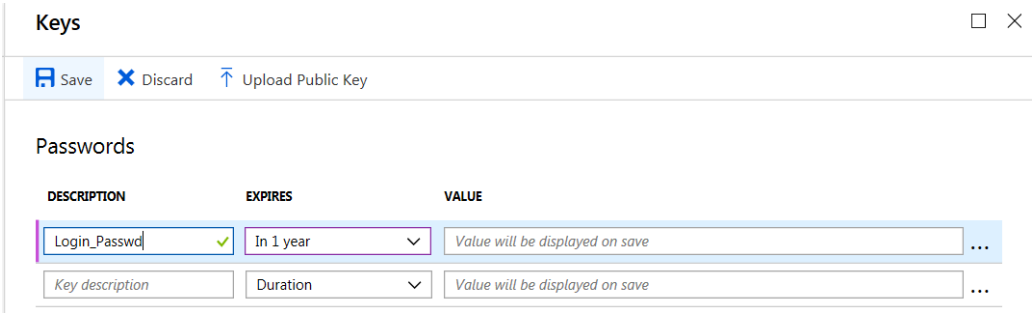
5. Click on the newly created **App**.
6. Click on **Settings**.



7. In the right panel, click on **Keys** to create a password.



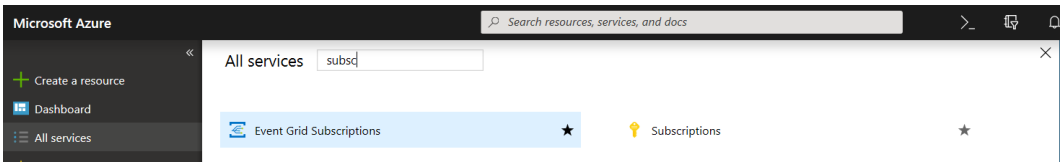
8. Click on **Save** to generate the password.



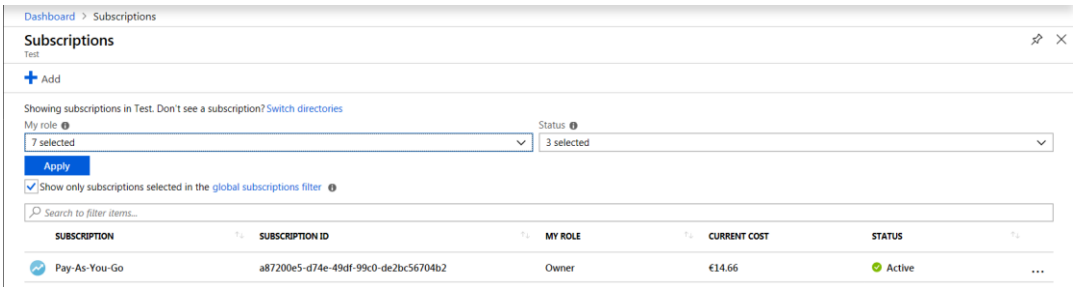
2.2 Grant Permissions

Now you need to set the permissions on your Azure subscriptions.

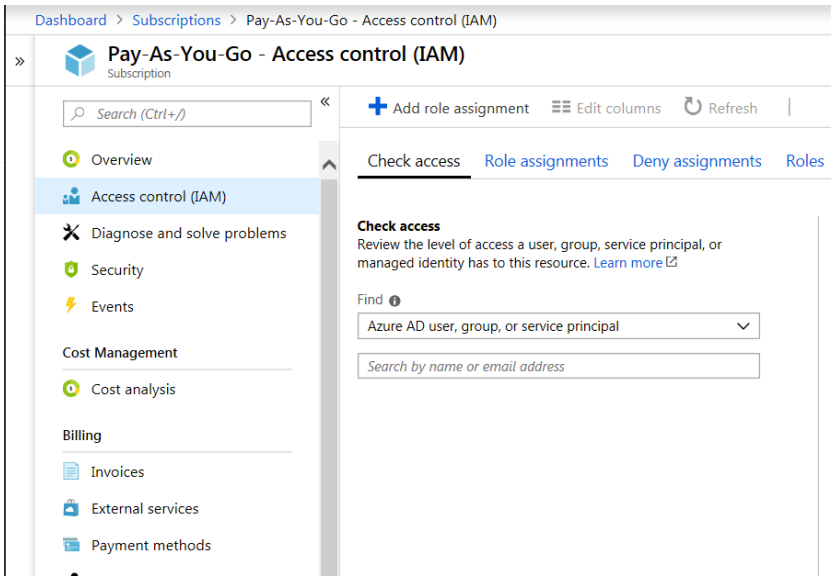
1. Go to **All services** in the left panel, search for **subscriptions**, and click on it.



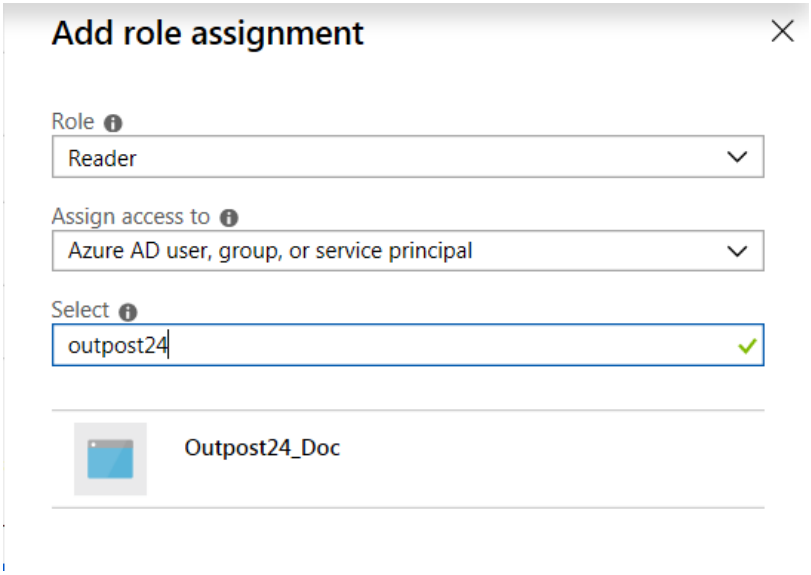
It lists all the subscriptions you have on Azure.



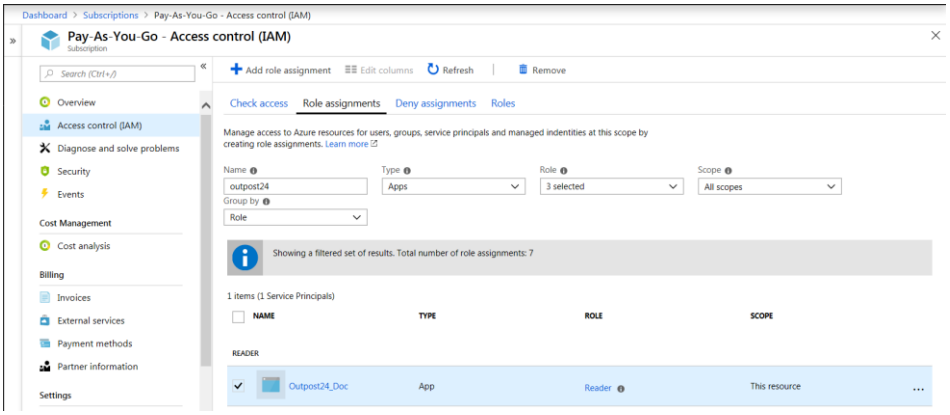
2. For every subscription you want EWP to manage, you need to:
   - Select the subscription.
   - Click on **Access Control panel** (IAM).
   - Click **Add role assignment.**



3. Add a **role assignment** of role “Reader” and select the Application of type WebApp/API (that has been created previously) as member.



4.Click **Save** to apply the changes.

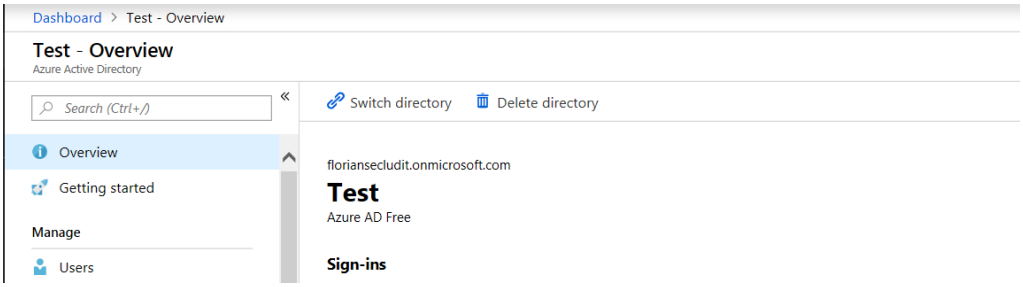


3 EWP Configuration

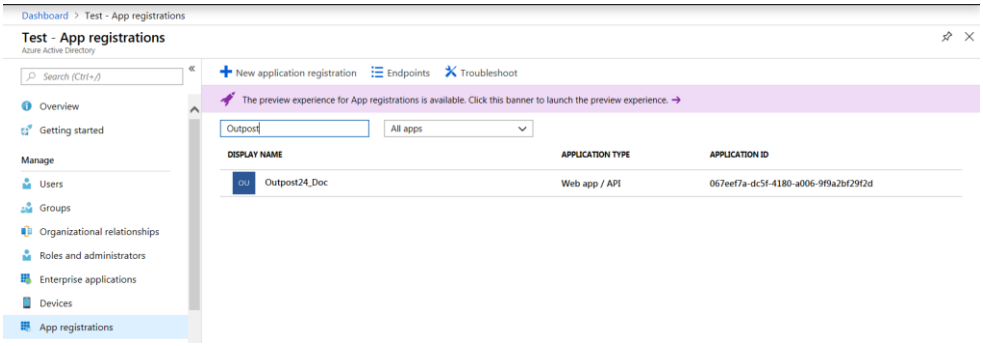
Enter you EWP account and configure Azure credentials using the following steps:

1. Go to **Inventory** on the bottom left panel.
2. Activate Azure Module (if not already activated and set to **ON**).
3. Click **Add Credentials.**

- **Tenant** and **Tenant ID**: Tenant ID is the name of your entry in Azure Active Directory. You need to provide the tenant of the active directory in which the app is registered as such XXX.onmicrosoft.com or the ID of the directory.



- **Client ID** and **User Name**: Client ID is the Application ID you created. You need to provide the client_id which is the application id created when you registered the app.



- **Secret** and **Password**: The password you choose while creating the **keys** of the application in the Active Directory.

4 Annex

The below table shows the required operations to run the CIS Azure Foundation Benchmark v1.0.0. In other terms, the list contains a set of operations that the service principal account shall be able to run (granted privileges). All granted privileges are READ only.

Service	Operation	Checks Dependencies
azure-mgmt-subscription	Subscriptions List	ALL
azure-graphrbac	Users List	1.1, 1.2, 1.3
azure.mgmt.authorization.	Role definitions List	1.1, 1.2, 1.23
azure.mgmt.authorization.	Role definitions List	1.1, 1.2, 1.23
azure.mgmt.authorization.	Role assignments List	1.1, 1.2
Security Center -Rest API	Auto provisioning settings List	2.2
Security Center -Rest API	Policies List	2.1, 2.3 – 2.19
Security Center -Rest API	Policies List	2.1, 2.3 – 2.19
azure.mgmt.storage	Storage accounts List	3.1, 3.2, 3.3, 3.6, 3.7
azure.mgmt.storage	Storage accounts List keys	3.7
azure.mgmt.storage	Blog containers List	3.7
azure-mgmt-monitor	Activity logs List	3.3
azure-mgmt-monitor	Log profiles List	5.1, 5.2
azure-mgmt-monitor	Activity log alerts List by resource group	5.3 – 5.12
azure-mgmt-monitor	Diagnostic settings List	5.13
azure-mgmt-sql	Servers List	4.2.1 – 4.2.8
azure-mgmt-sql	Databases List by server	4.2.1 – 4.2.8
azure-mgmt-sql	Database auditing settings Get	4.2.1 – 4.2.8
azure.mgmt.resource. resources	Resource groups List	5.3 – 5.12, 7.1, 7.2, 7.4, 7.6, 8.3
azure.mgmt.keyvault	Vaults List	5.13, 8.1, 8.2

azure.mgmt.network	Network security groups List all	6.1, 6.2
azure.mgmt.network	Network watchers Get flow log status	6.4
azure.mgmt.network	Network watchers List all	6.4, 6.5
azure.mgmt.compute	Disk List	7.3
azure.mgmt.compute	Virtual machines List	7.1 – 7.4, 7.6
Key Vaults – Rest API	Get keys Get keys	8.1
azure.mgmt.resource.locks	Management locks List at resource group level	8.3
Powershell – Sql server	Get-AzureRmSqlServer	4.1.1 – 4.1.8, 6.3
Powershell – Sql server	Get-AzureRmSqlServerAuditing	4.1.1, 4.1.6
Powershell – Sql server	Get-AzureRmSqlServerThreatDetectionPolicy	4.1.2 - 4.1.5, 4.1.7
Powershell – Sql server	Get-AzureRmSqlServerFirewallRule	6.3
Powershell – Sql server	Get-AzureRmSqlServerActiveDirectoryAdministrator	4.1.8
Powershell – Active Directory	Get-MsolUser	1.1, 1.2

***Note**: You need to create a service principal account on Azure to run the benchmark.*