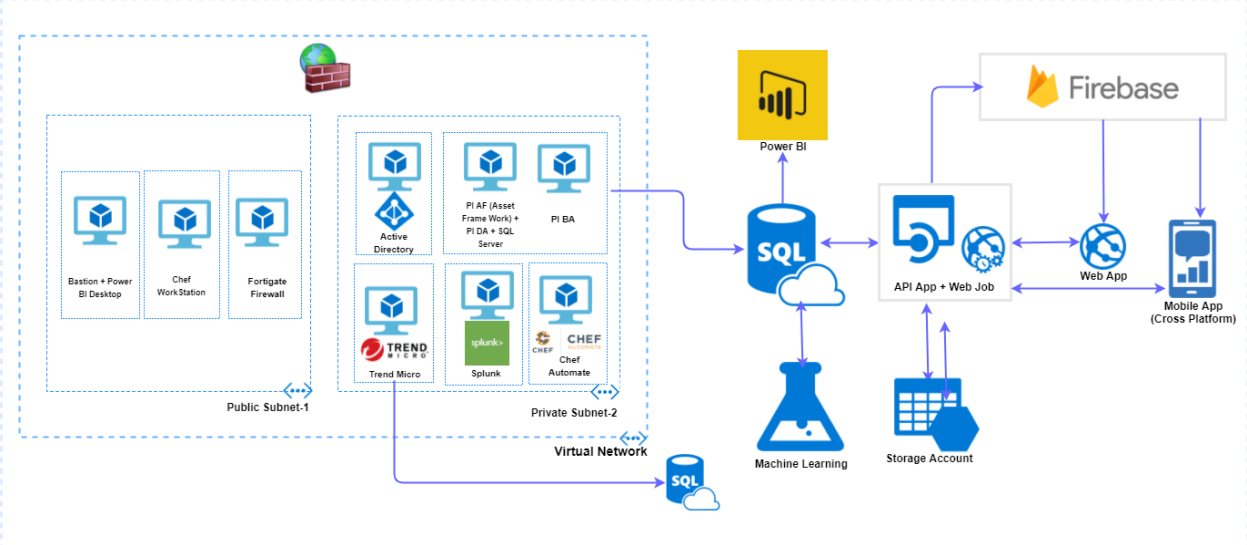
Internet of Things Automation

User Guide

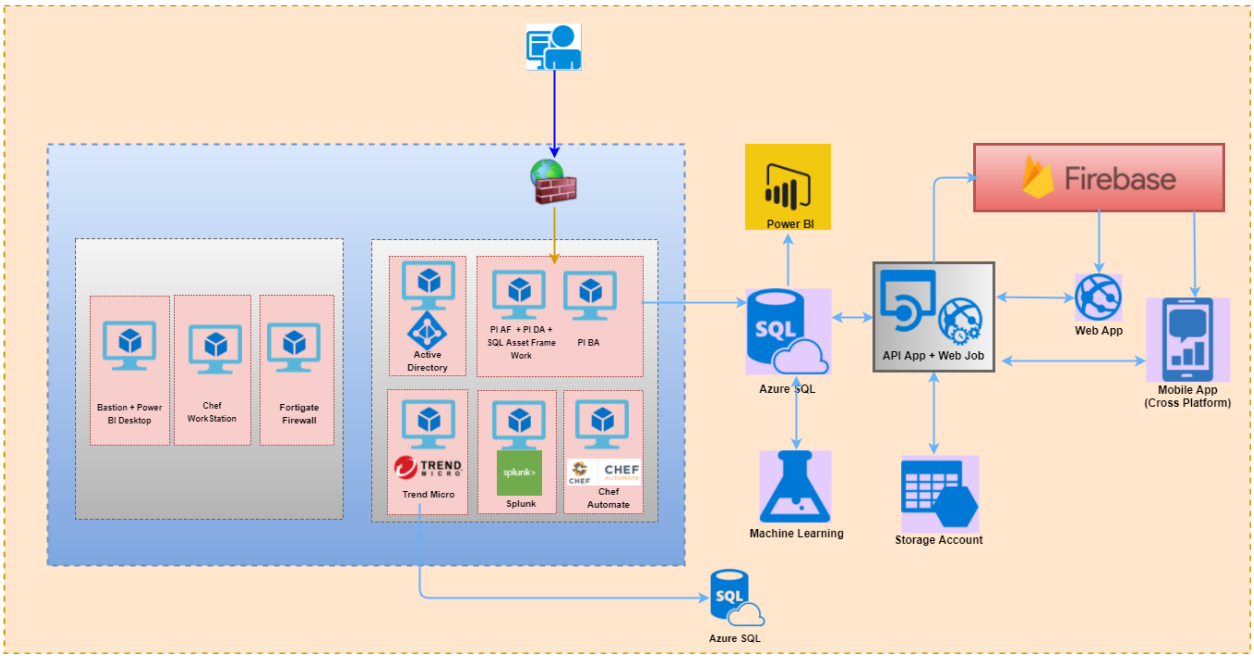
SYSGAIN, INC.

Contents

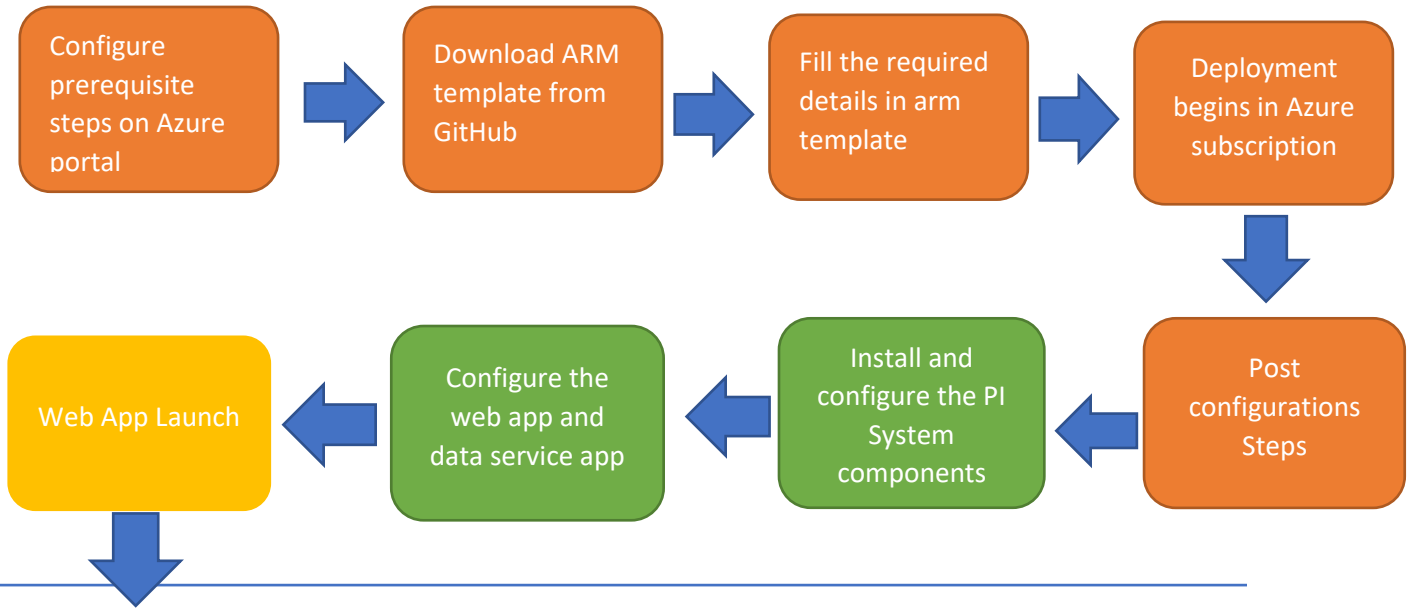
1. Architecture



1.1. Data Flow Architecture Diagram



2. High Level Deployment Process to be Followed



3. Deployment Costs

VM Name	VMSize	OS	Software Cost	Azure Cost/Hour	Azure Cost/Month
Bastion Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2012 R2	PAYG	` $ 0.21/Hour	$98.95/Month
Chef Automate Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL (license $137node/annual)	$ 0.14/Hour	$197.90/Month
Active Directory Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2016	PAYG	$ 0.21/Hour	$197.90/Month
Chef workstation	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2012 R2	PAYG	$ 0.21/Hour	$197.90/Month
PIAFSQL Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2016 + SQL 2016SP1	BYOL	$0.61/Hour	$98.95 /Month
PIBAVM Server	Standard DS4 v2 (8 cores, 28 GB memory)	Windows 2012 R2	BYOL	$ 0.84/Hour	$790.87/Month

Splunk Server	Standard DS2 v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	$ 0.14/Hour	$159.22/Month
Trend Micro	Standard DS2 v2 (2 cores, 7 GB memory)	CentOS 7	BYOL	$ 0.14/Hour	$159.22/Month
Web App	S1 Standard (1 instance)			$ 0.1/Hour	$279.74/Month
API App	S1 Standard (1 instance)			$ 0.1/Hour	$279.74/Month
FortiGate Firewall	Standard D2 v2 (2 core, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	$ 0.14/Hour	$104.16/Month
Machine Learning	S1 Standard			$1 per studio experimentation/ hour	$9.99 per seat/month

Note: The above mentioned VM Sizes are the default values, User can change the values based on his instance profile. For BYOL the software costs are additional and could be found on the respective product pages

3.1. SERVER DETAILS

S.NO	Server Name	Abbreviation	Purpose
1	PIAFSQL Server	PI Assert Framework	On this server we will install ULF Connector, AF Server, DA Server
2	PIBA Server	PI Business Analytics	On this server we install BA Installation and config PIBAVM Server
3	Chef Automate	Chef Automate	It provides a dashboard which is used to view all nodes and compliance of the nodes, In this we run chef automate

4	Chef Workstation	Chef Workstation	User will user to bootstrap, managing and applying cookbooks to all the nodes
5	PIDA Server	PI Data Archive	This installation we do in PIAFSQL Server

4. Prerequisites

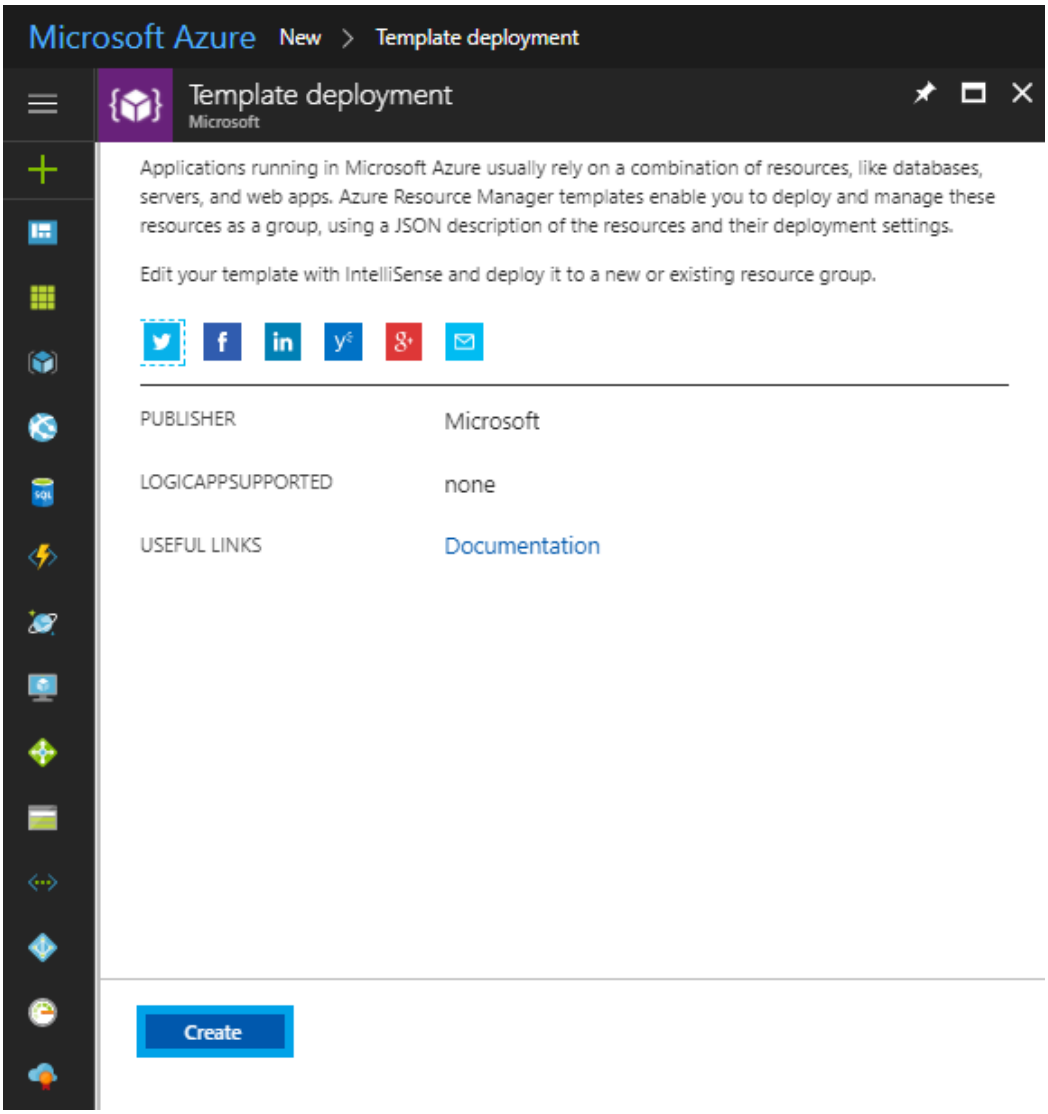
1. Launching Firewall Template
2. The Azure AD B2C Tenant should be created and register your web application.
3. Create an account in Power BI.
4. Dynatrace account creation in SAAS.

4.1 Launching Firewall Template

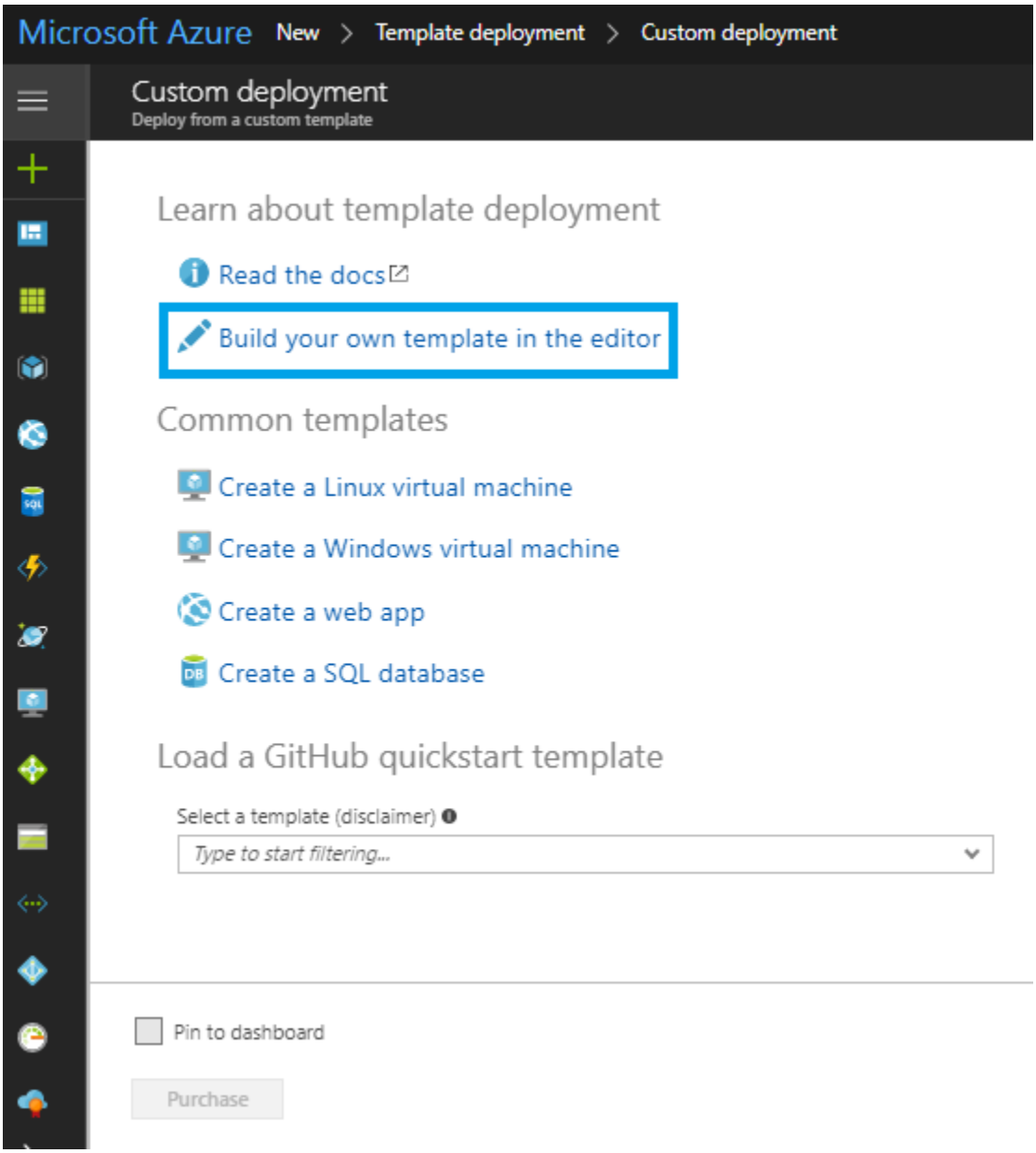
Go to the following GitHub repo: https://github.com/sysgain/iot-automation/tree/sysgainiot

Copy the "fortigate-main-template.json" file.

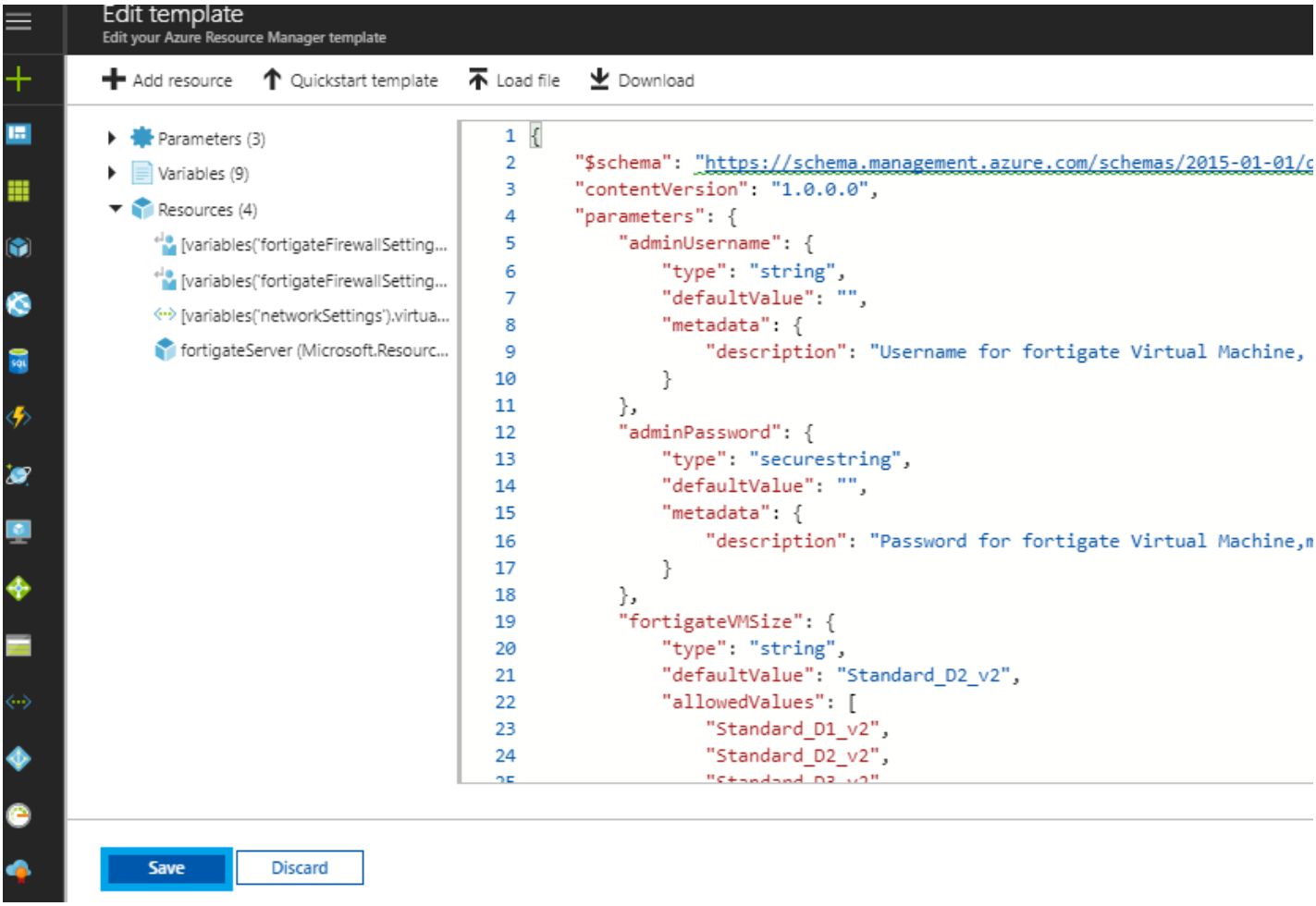
1. Open Azure portal, Navigate to **New (+)**, search for **Template deployment,** then click on **Create.**



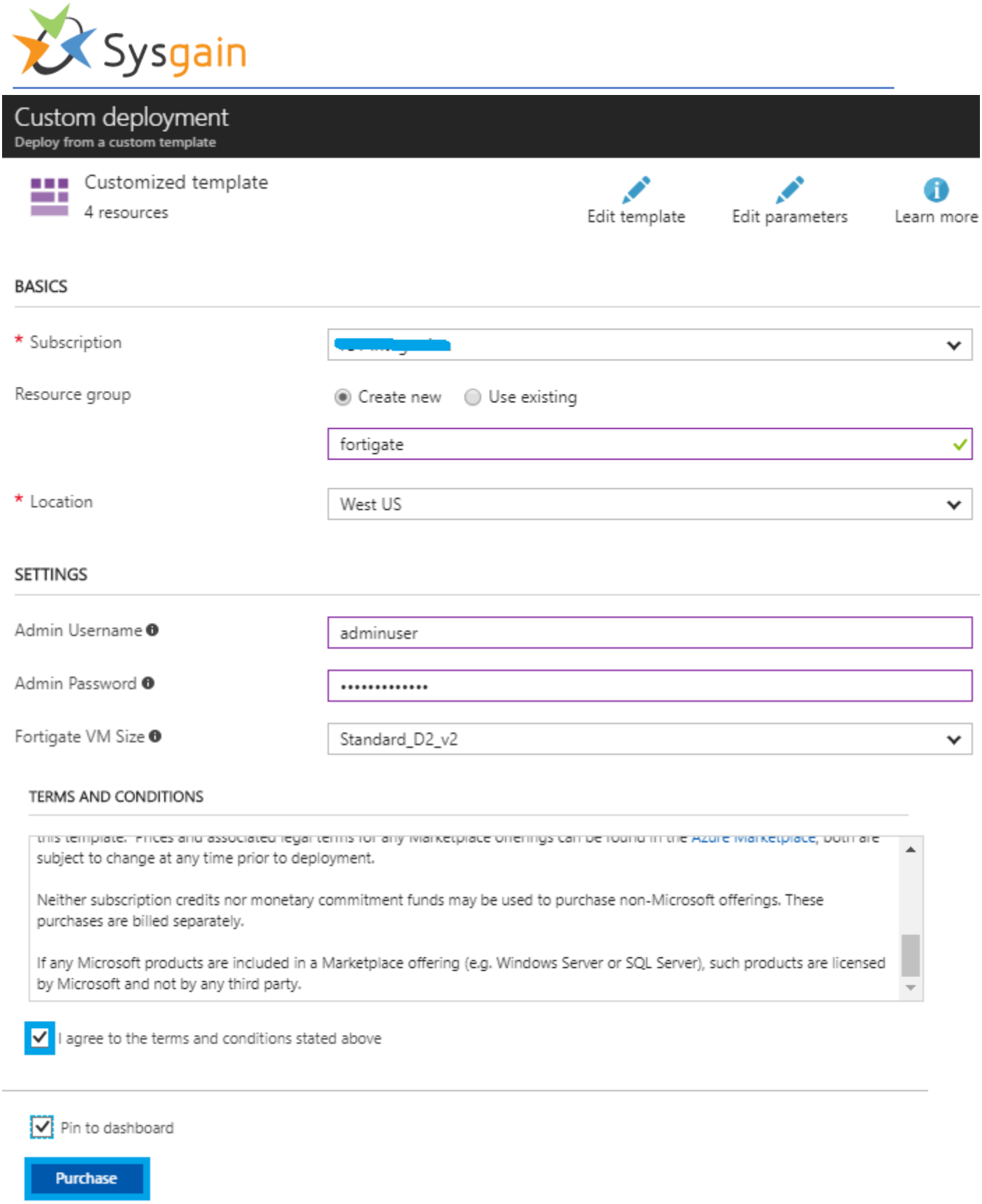
2. Click on **Build your own Template**.



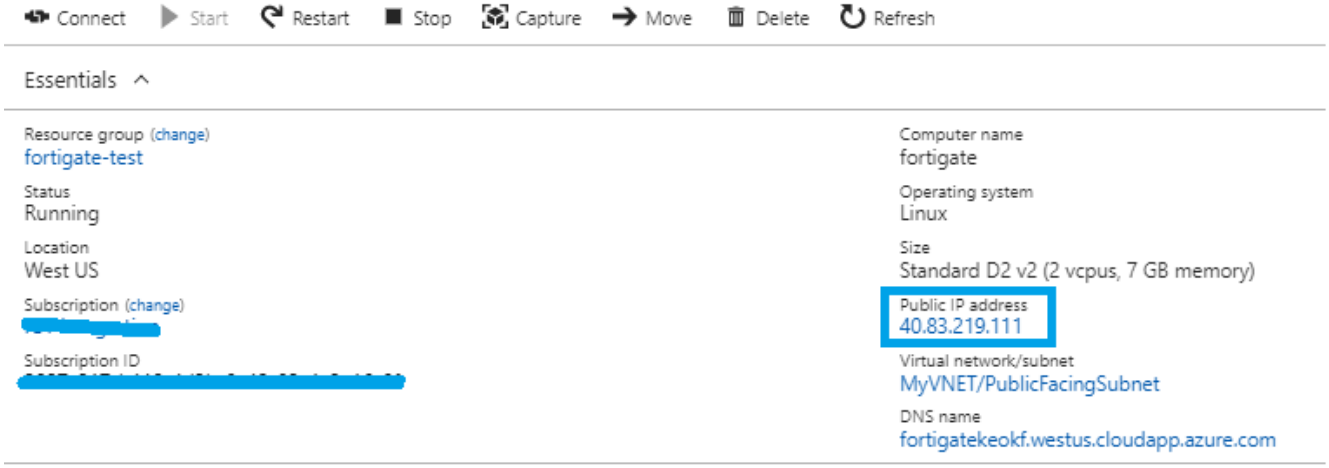
3. Paste the template you copied from the JSON file and click on **Save**.



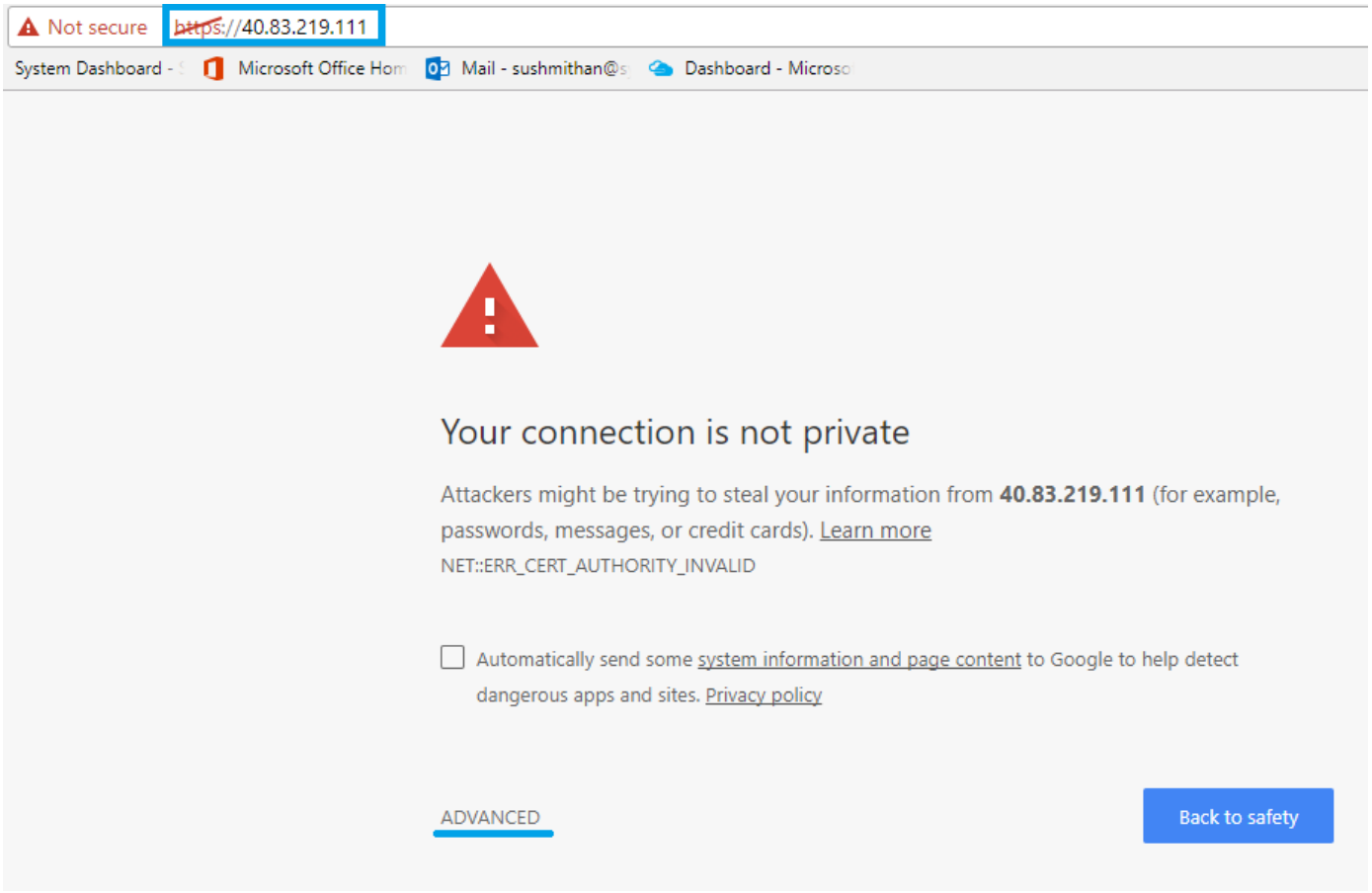
4. Fill out the Resource Group Name, Location, Admin username, and Admin password fields, then select the Fortigate vm size
5. After all the parameters are entered, check the terms and conditions box and click on **Purchase**.


Custom deployment
Deploy from a custom template
Customized template
4 resources
Edit template
Edit parameters
Learn more
BASICS
* Subscription
Resource group
Create new
Use existing
fortigate
* Location
West US
SETTINGS
Admin Username
adminuser
Admin Password
Fortigate VM Size
Standard_D2_v2
TERMS AND CONDITIONS
subject to change at any time prior to deployment.
Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.
If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.
I agree to the terms and conditions stated above
Pin to dashboard
Purchase

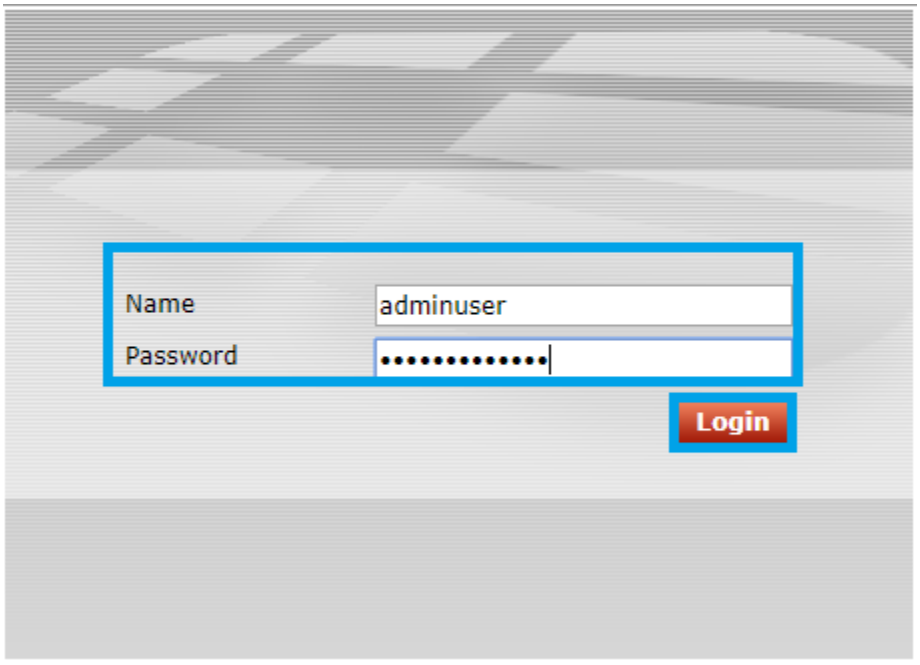
6. After deploying the template, go to the Fortigate Virtual Machine resource in the Resource Group. Click on that resource, then copy the IP address.



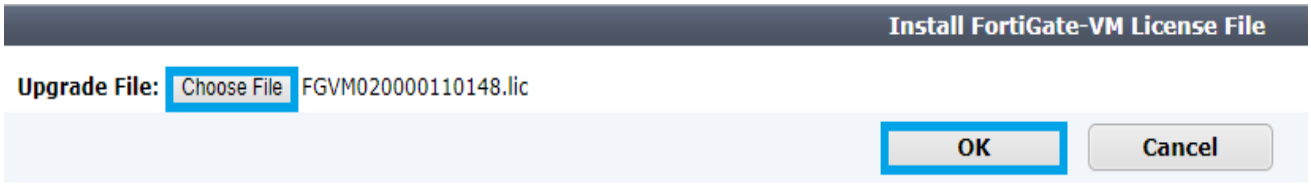
7. Paste the IP address in a new browser. When the security alert pops up, click on Advanced.



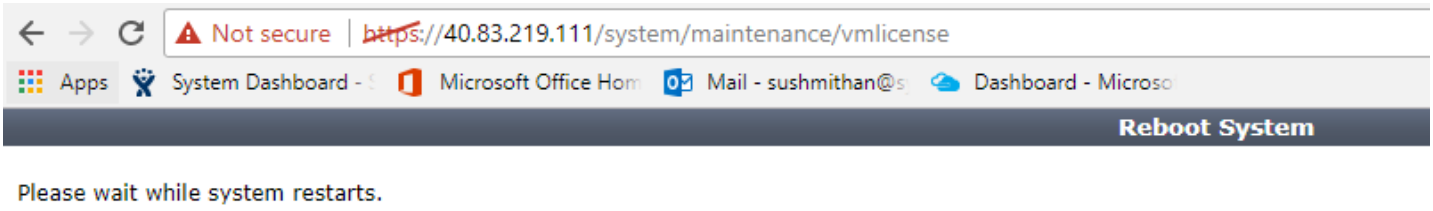
8. The login popup box will appear. Give the admin username and admin password that you provided in the parameter section. Then click on Login.



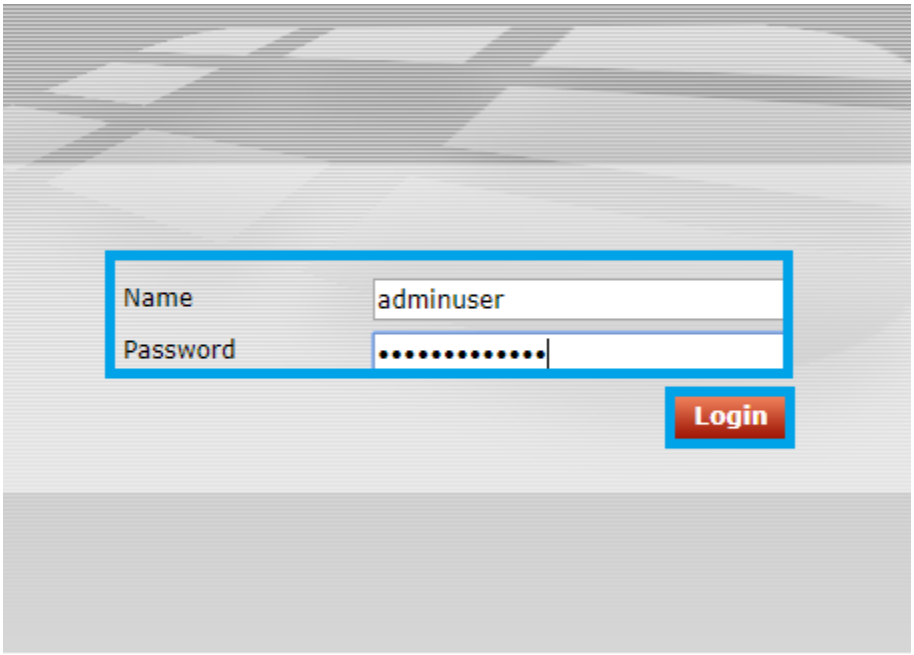
9. After logging in, you will see the "Install Fortigate-VM License File" page. If you already have the fortigate license file from OSI Soft, click the "Choose File" button and navigate to that file in the dialogue box and appears. If you don't have the license file, contact OSI Soft at https://techsupport.osisoft.com/Downloads/All-Downloads .You may need to create an account.



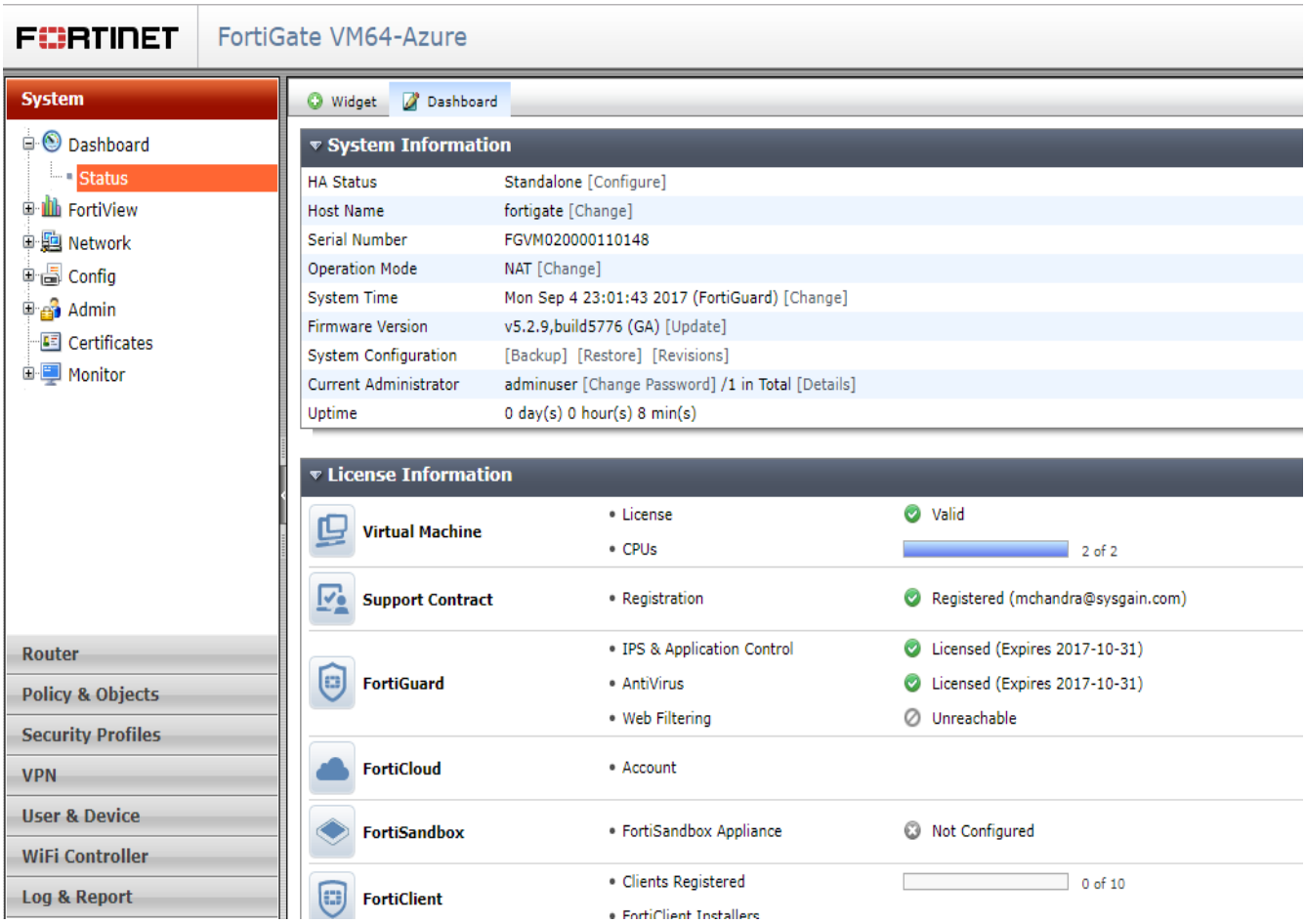
10. After this, the system will automatically restart. It may take up to 15 minutes.



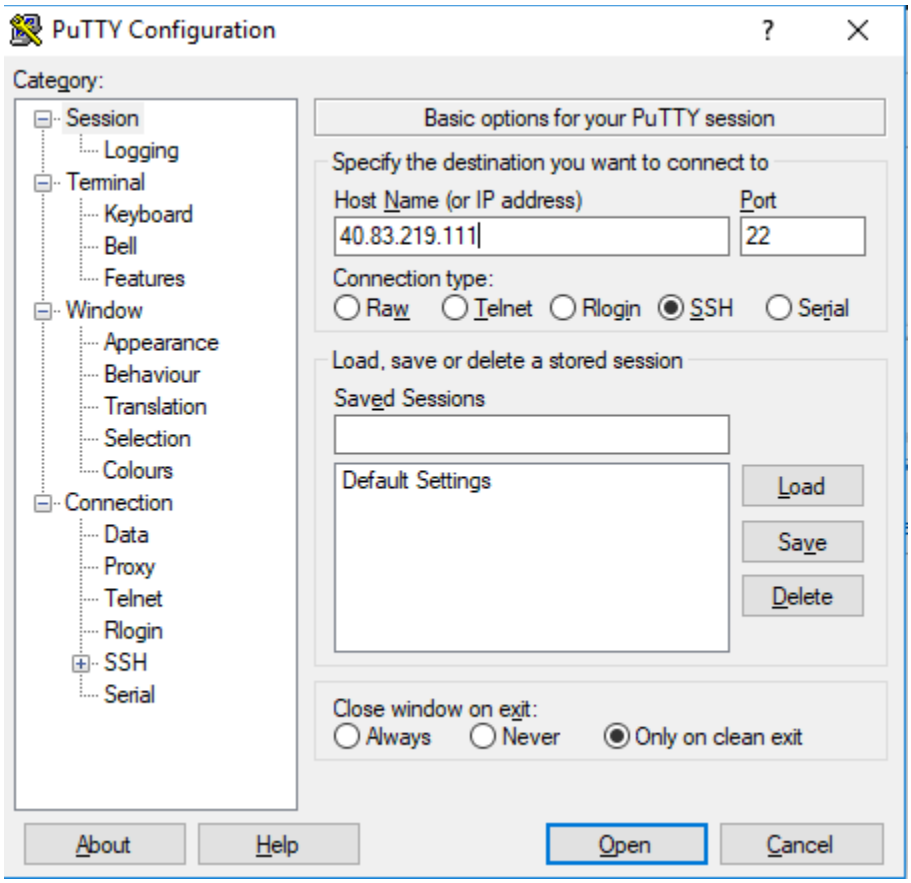
11. After reboot, the system will again ask for username and password. Provide them again.



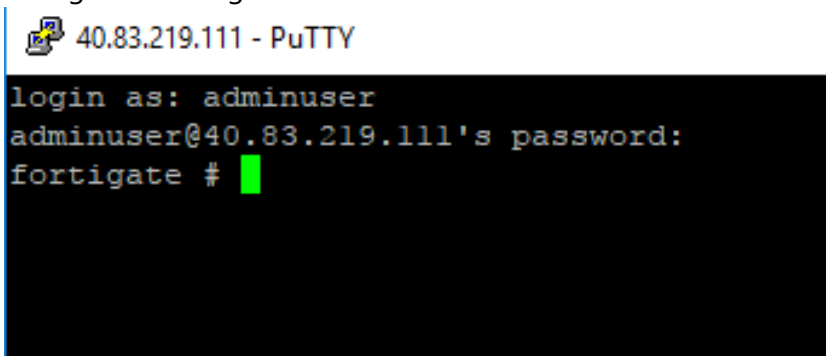
12. After logging in, you will find yourself on the Fortigate dashboard site. Go to Status, where you can check if the license file is valid. It should appear as valid.


FORTINET
FortiGate VM64-Azure
System
Dashboard
Status
FortiView
Network
Config
Admin
Certificates
Monitor
Router
Policy & Objects
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
Widget
Dashboard
System Information
HA Status
Standalone [Configure]
Host Name
fortigate [Change]
Serial Number
FGVM020000110148
Operation Mode
NAT [Change]
System Time
Mon Sep 4 23:01:43 2017 (FortiGuard) [Change]
Firmware Version
v5.2.9,build5776 (GA) [Update]
System Configuration
[Backup] [Restore] [Revisions]
Current Administrator
adminuser [Change Password] /1 in Total [Details]
Uptime
0 day(s) 0 hour(s) 8 min(s)
License Information
Virtual Machine
License
Valid
CPUs
2 of 2
Support Contract
Registration
Registered (mchandra@sysgain.com)
FortiGuard
IPS & Application Control
Licensed (Expires 2017-10-31)
AntiVirus
Licensed (Expires 2017-10-31)
Web Filtering
Unreachable
FortiCloud
Account
FortiSandbox
FortiSandbox Appliance
Not Configured
FortiClient
Clients Registered
0 of 10

13. After that, open PuTTY and enter the Fortigate Virtual Machine IP address in Host name. Click on Open.



14. Log in with your admin username and admin password (as provided in the parameter section), then navigate to Fortigate as shown below.



15. Enter the below commands line by line, being careful not to include any errors. You are adding a public subnet to the Fortigate Virtual Machine.

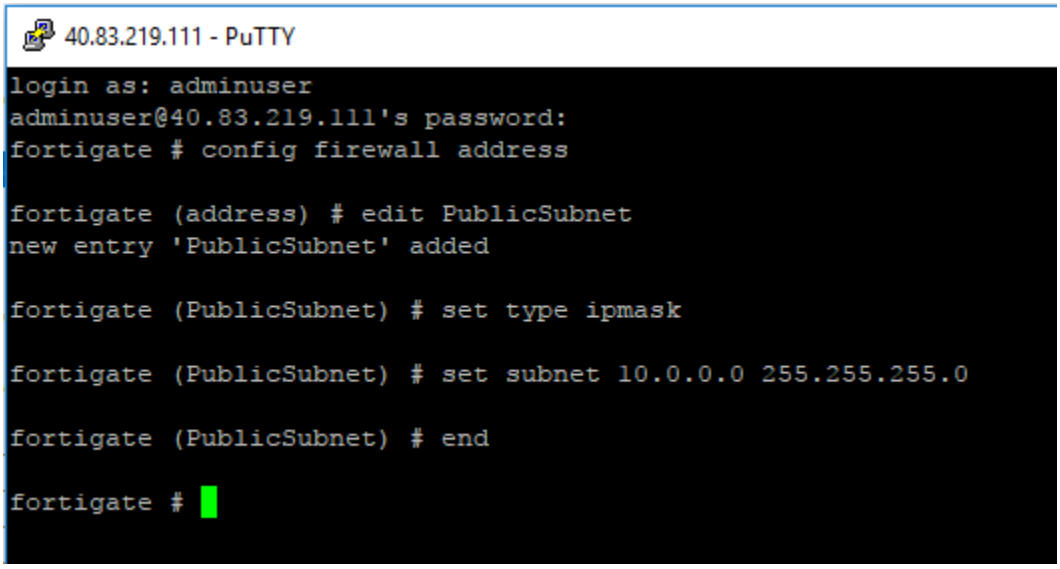
config firewall address

edit PublicSubnet

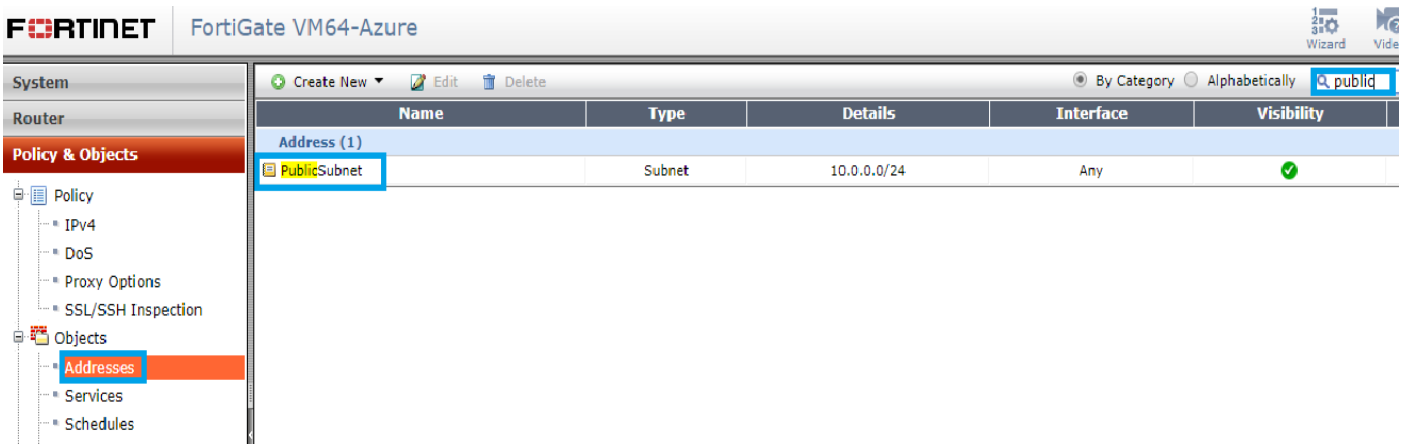
set type ipmask

set subnet 10.0.0.0 255.255.255.0

end



16. Return to the Fortigate dashboard and navigate to **Policy & Objects**. Go to Addresses search for publicsubnet , you can check the if Public subnet is added or not.

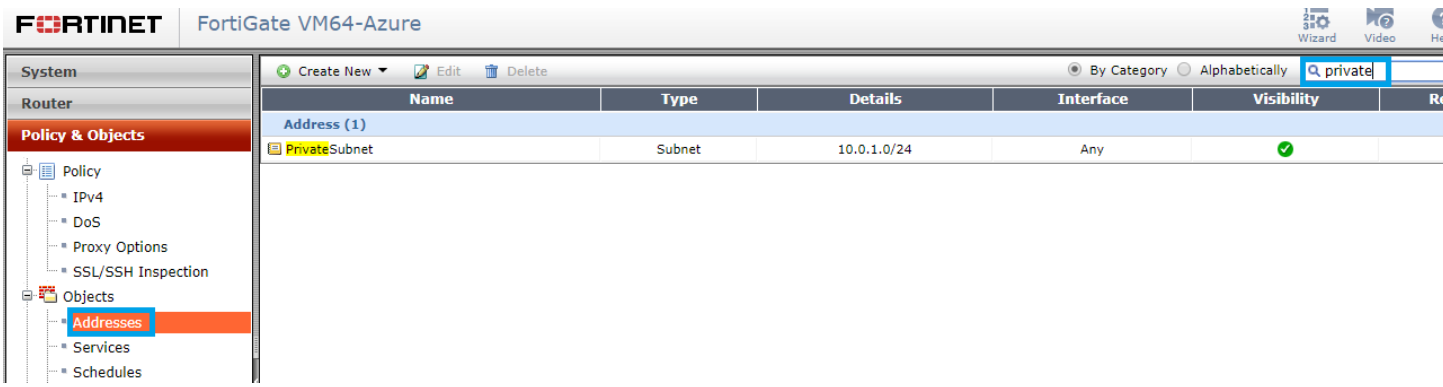


17. Go the PuTTY and enter the following commands line by line. Here you are configuring the public subnet to a private subnet.
    config firewall address
    edit PrivateSubnet
    set type ipmask
    set subnet 10.0.1.0 255.255.255.0

end

```
fortigate # config firewall address

fortigate (address) # edit PrivateSubnet
new entry 'PrivateSubnet' added

fortigate (PrivateSubnet) # set type ipmask

fortigate (PrivateSubnet) # set subnet 10.0.1.0 255.255.255.0

fortigate (PrivateSubnet) # end

fortigate #
```

18. Navigate to the Policy & Objects > Objects > Addresses in the Fortigate VM to double check that the public subnet changed to a private subnet.



19. Go to PuTTY, then enter the below commands to configure the firewall policy.

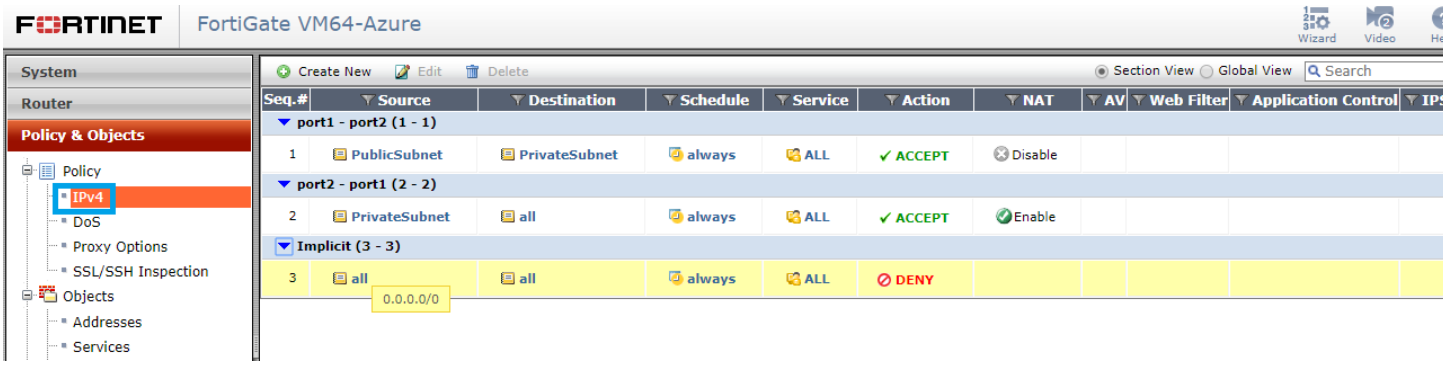
config firewall policy
edit 2
set action accept
set dstaddr all
set dstintf port1
set srcaddr PrivateSubnet
set srcintf port2
set nat enable
set natip 10.10.0.4 255.255.255.0
set service ALL
set schedule always
end

config firewall policy
edit 3
set srcintf port1
set srcaddr PublicSubnet
set dstintf port2
set dstaddr PrivateSubnet
set service ALL
set schedule always
set action accept
end

```
fortigate # config firewall policy

fortigate (policy) # edit 2
new entry '2' added

fortigate (2) # set action accept

fortigate (2) # set dstaddr all

fortigate (2) # set dstintf port1

fortigate (2) # set srcaddr PrivateSubnet

fortigate (2) # set srcintf port2

fortigate (2) # set nat enable

fortigate (2) # set natip 10.10.0.4 255.255.255.0

fortigate (2) # set service ALL

fortigate (2) # set schedule always

fortigate (2) # end
```

```
fortigate # config firewall policy

fortigate (policy) # edit 3
new entry '3' added

fortigate (3) # set srcintf port1

fortigate (3) # set srcaddr PublicSubnet

fortigate (3) # set dstintf port2

fortigate (3) # set dstaddr PrivateSubnet

fortigate (3) # set service ALL

fortigate (3) # set schedule always

fortigate (3) # set action accept

fortigate (3) # end

fortigate #
```

20. Return to the Fortigate virtual machine in browser and navigate to the **IPv4** section in **Policy & Objects** you can see the Source, Destination, Service, Action, and NAT updated as per the above commands.

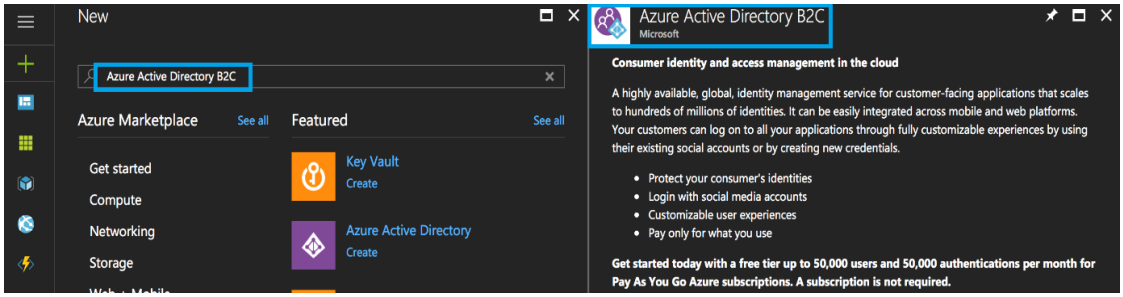


4.2. Azure B2C Tenant Creation and Configuration

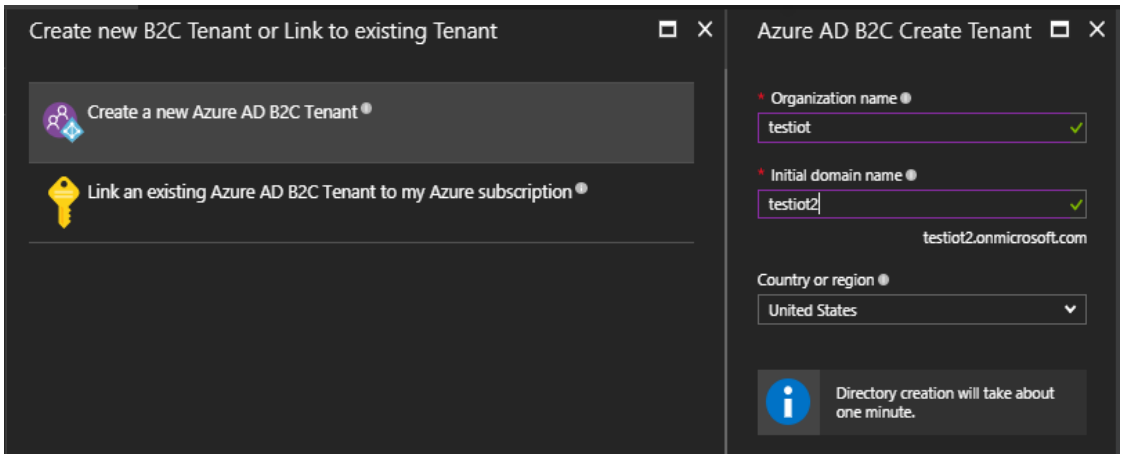
Creating Azure AD B2C tenant is a one-time activity, if you have a B2C Tenant already created by your admin then you should be added into that tenant as Global Administrator to register your app to get the B2C tenant id, application id and sign-in/sign-up policies.

Follow Below steps to create Azure AD B2C Tenant:

1. Create a new B2C tenant in **Azure Active Directory B2C**. You'll be shown a page with the information on Azure Active Directory B2C. Click **Create** at the bottom to start configuring your new Azure Active Directory B2C tenant.

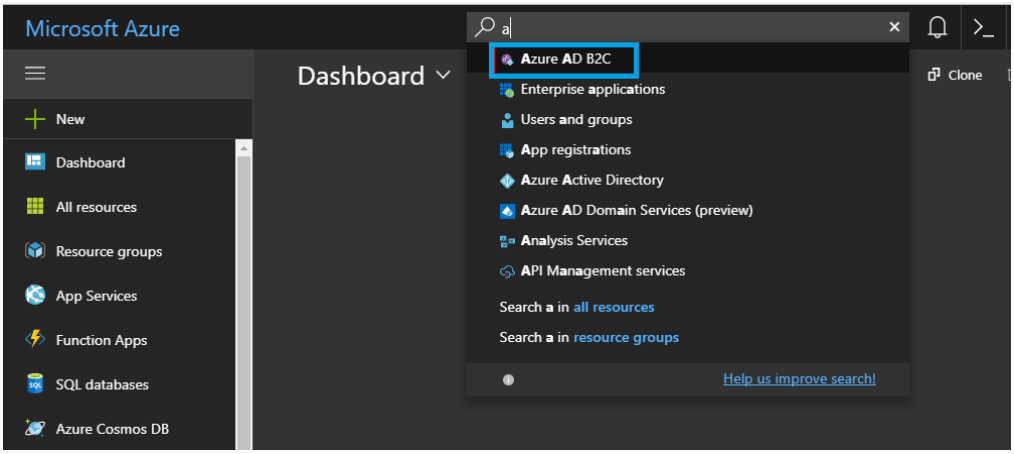


2. Choose the **Organization name**, **Initial Domain name** and **Country of Region** for your Tenant.

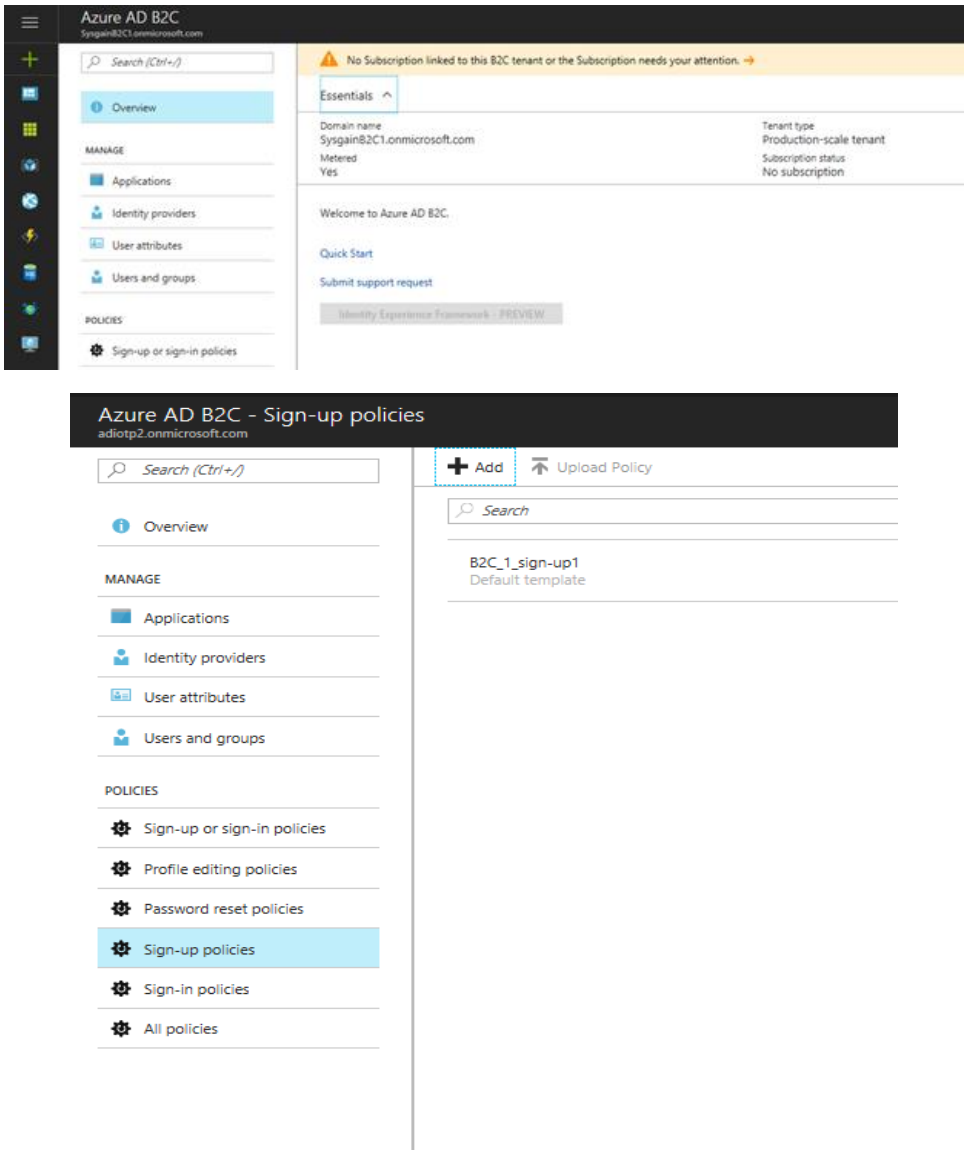


3. Once the B2C Tenant is created, you will see the below confirmation under the portal login user name.

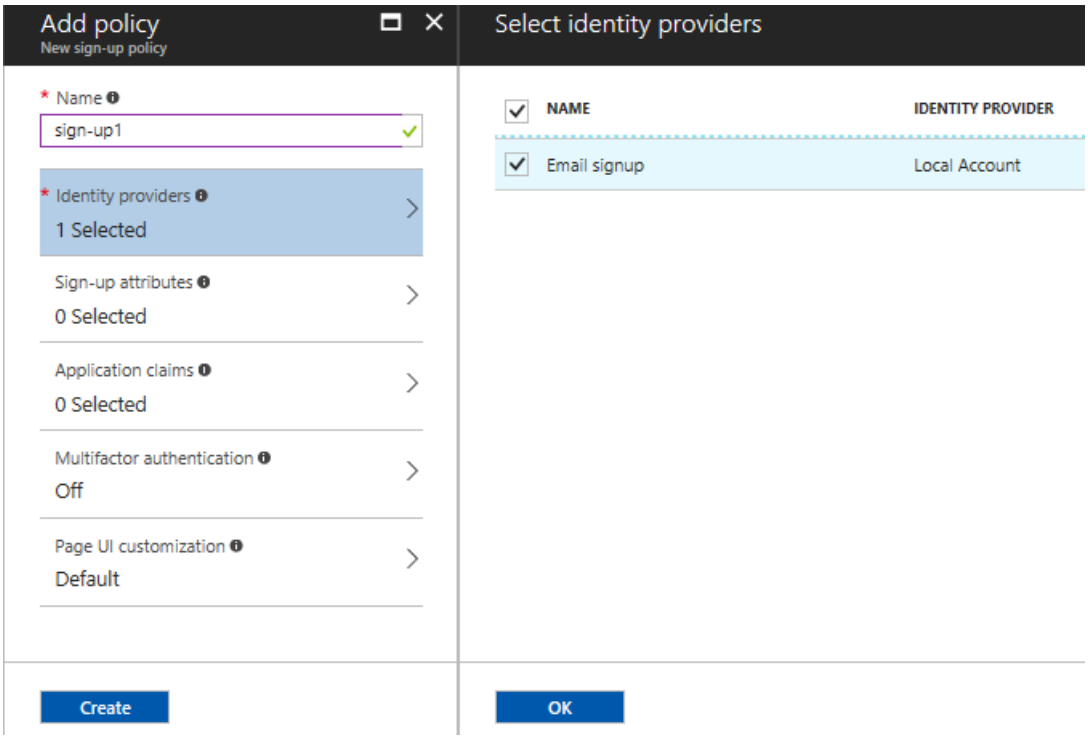
4. Switch to your created tenant by clicking on Created tenant under signout. Type Azure in search column select and click on Azure AD B2C.



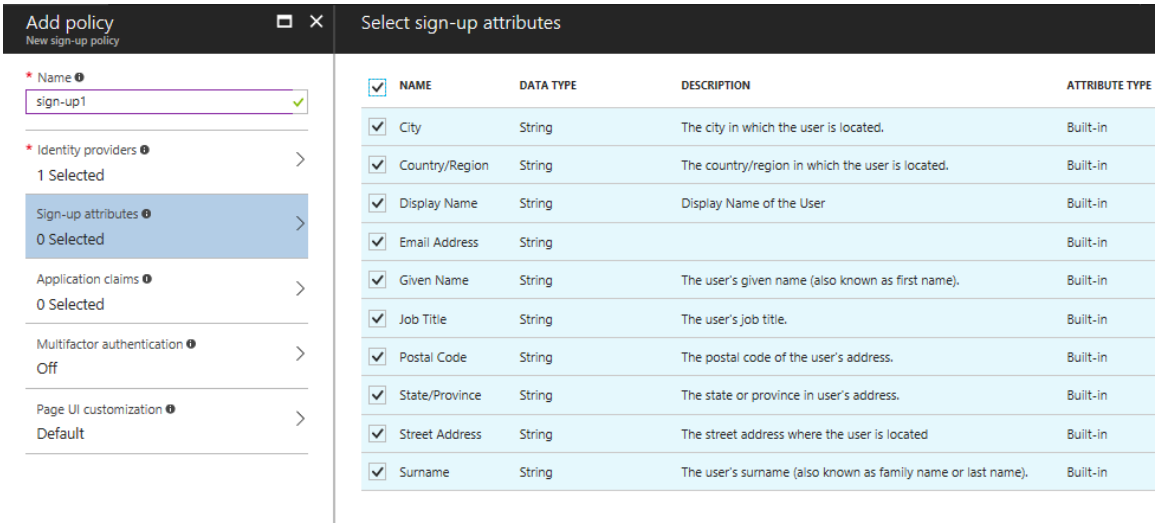
5. You can see the created tenant overview like below in that click on **Sign-up policies**. Then click on **Add** to add policy



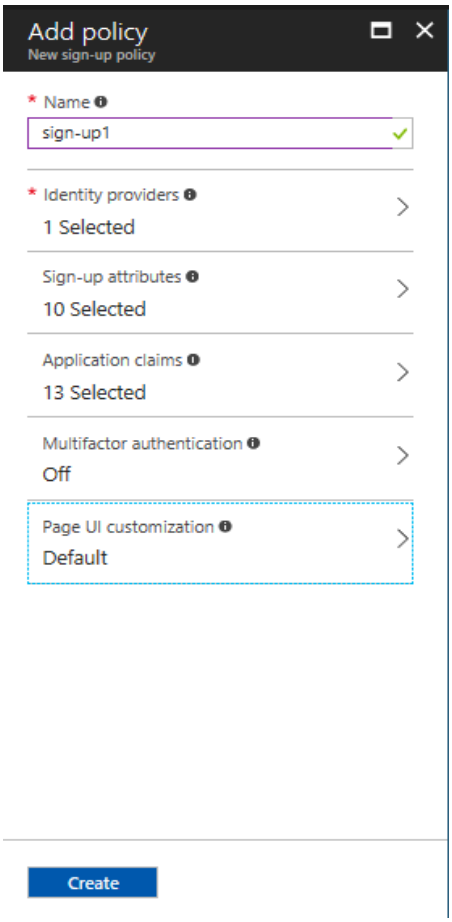
6. Provide the name and enter the details as shown below.



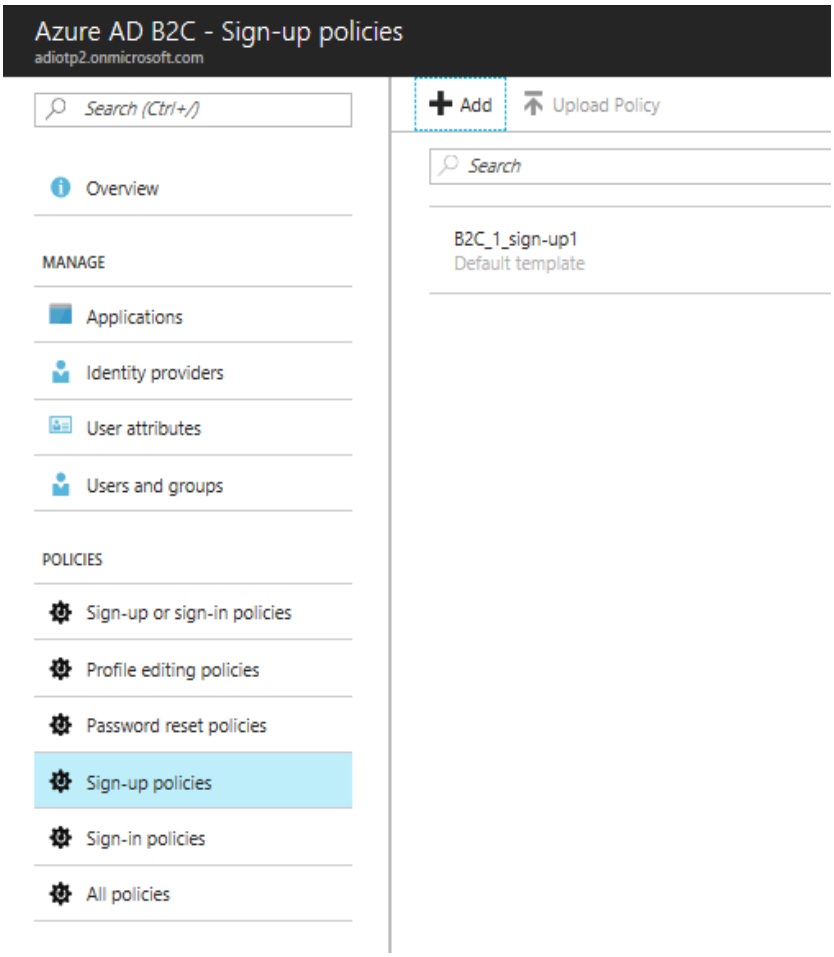
7. Select all the **Sign-up attributes** as show below.



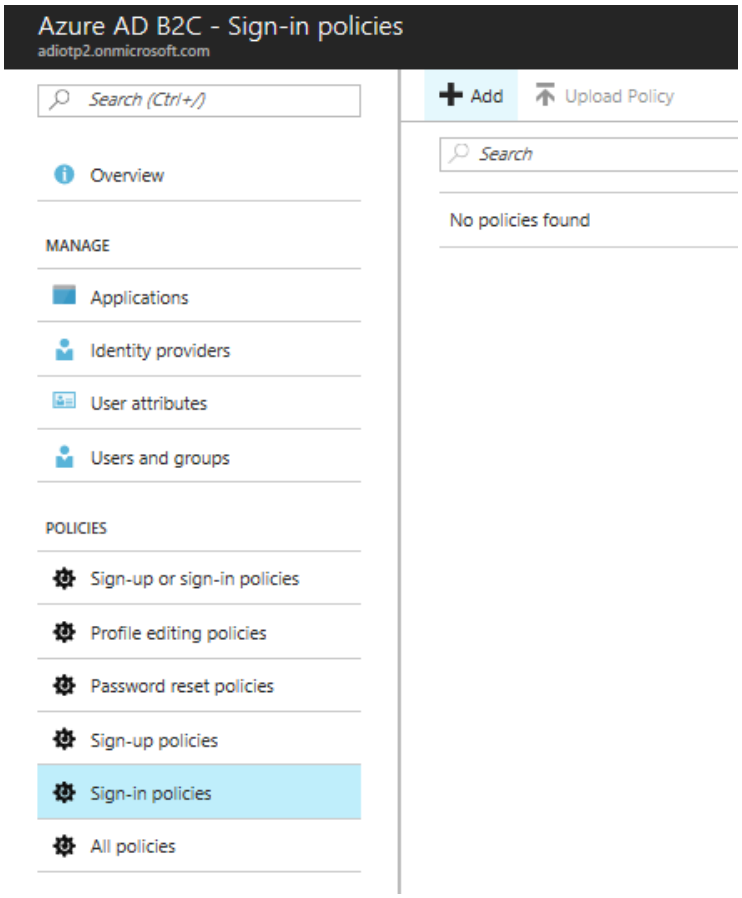
8. After filling all the required details, click on **Create**.


Add policy
New sign-up policy
* Name
sign-up1
* Identity providers
1 Selected
Sign-up attributes
10 Selected
Application claims
13 Selected
Multifactor authentication
Off
Page UI customization
Default
Create

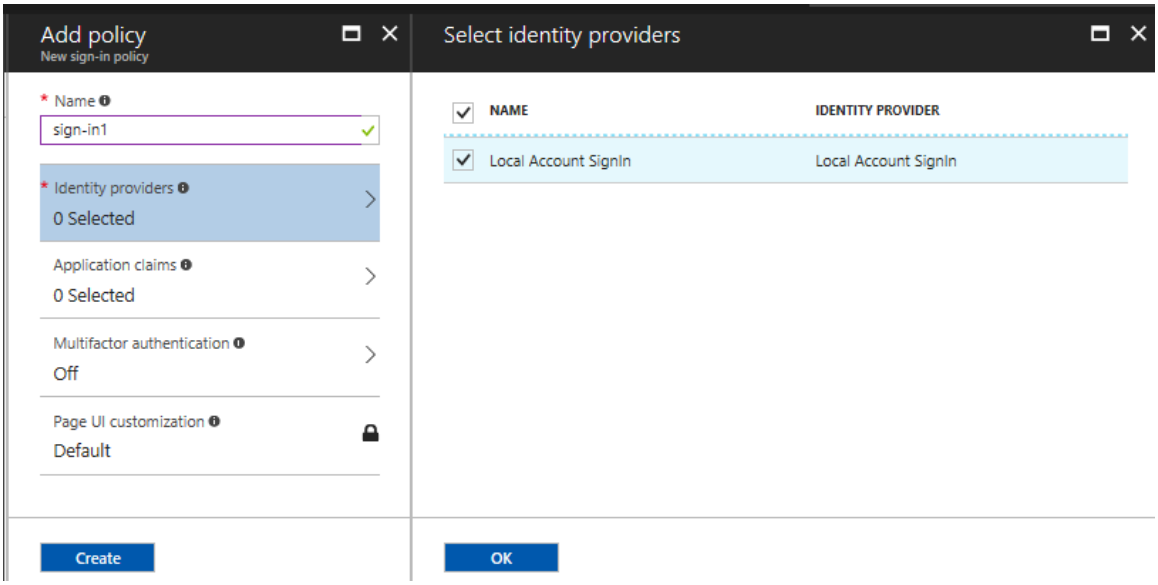
Once the deployment is complete, the below screen will appear with sign-up details.



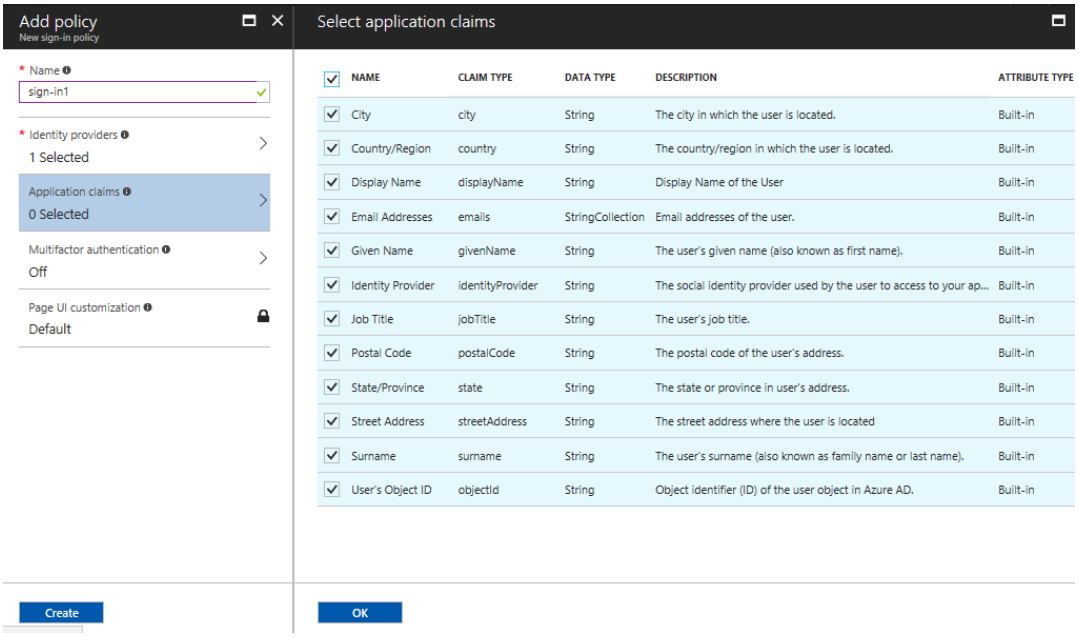
9. Click on **Sign-in policies**, then **Add**.



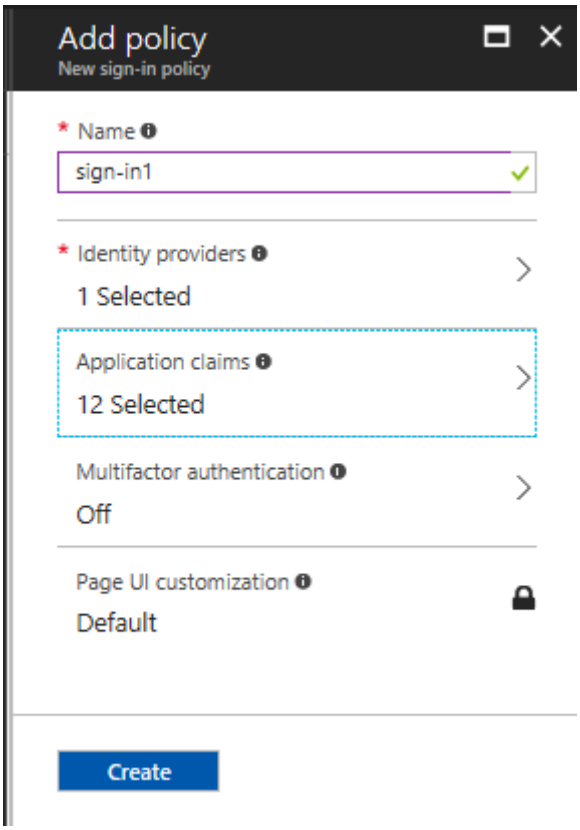
10. Provide a name and fill in the details as shown below.



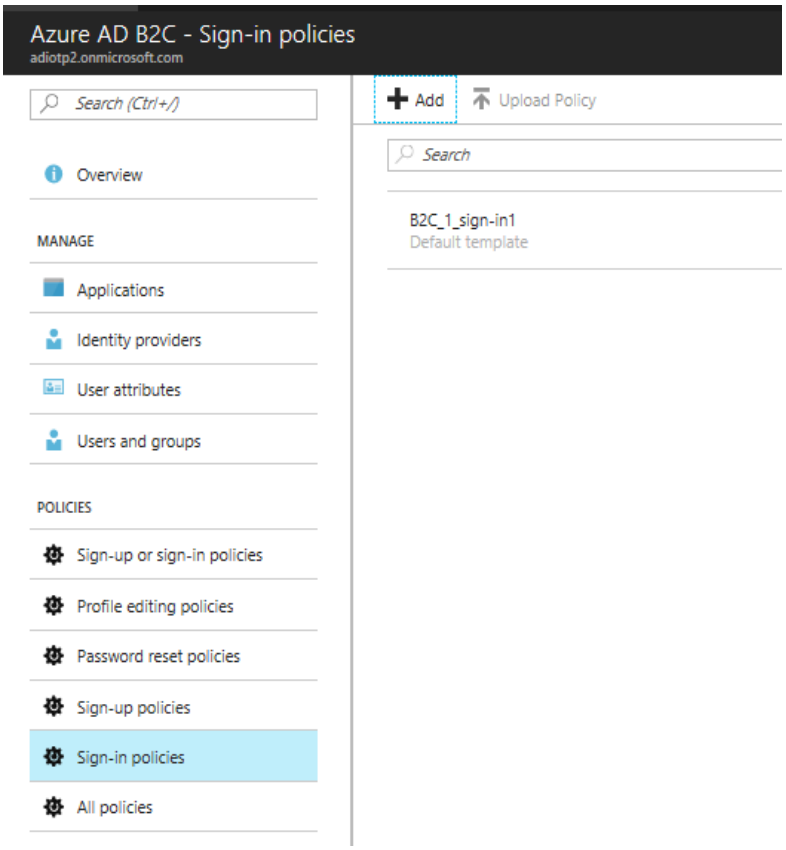
11. Select all **Application claim**



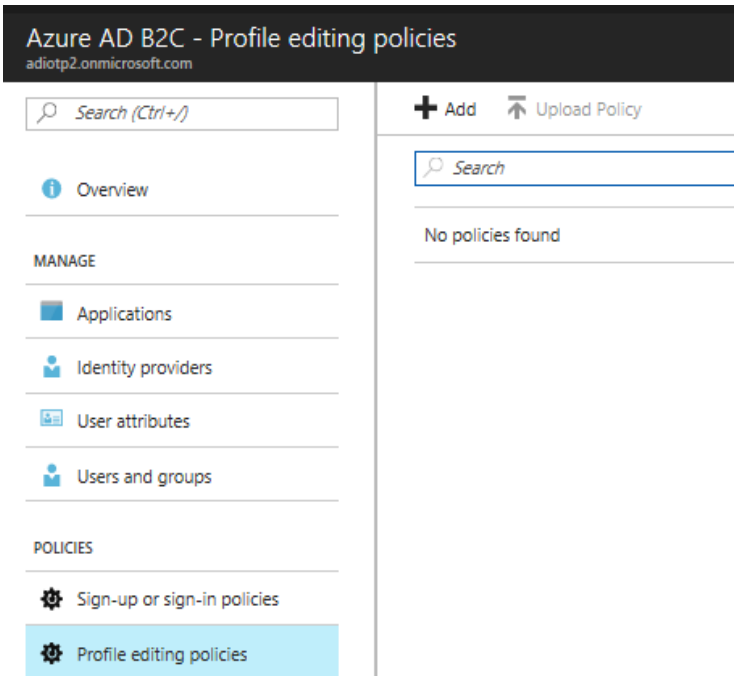
12. Once done, click on **Create**.



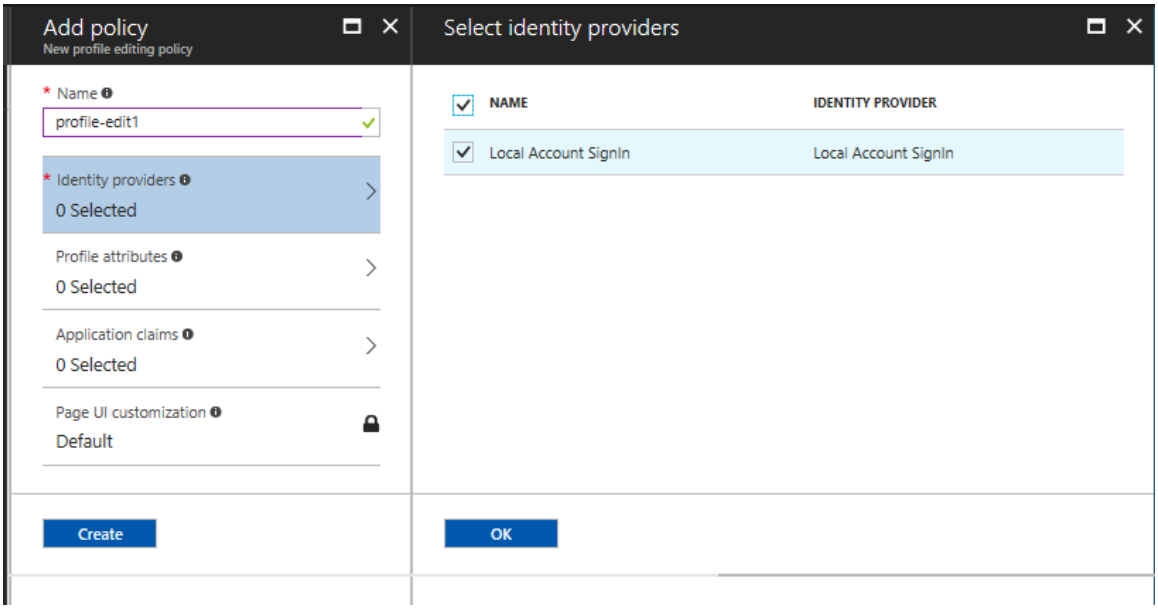
13. After deployment completes, the below screen will appear.



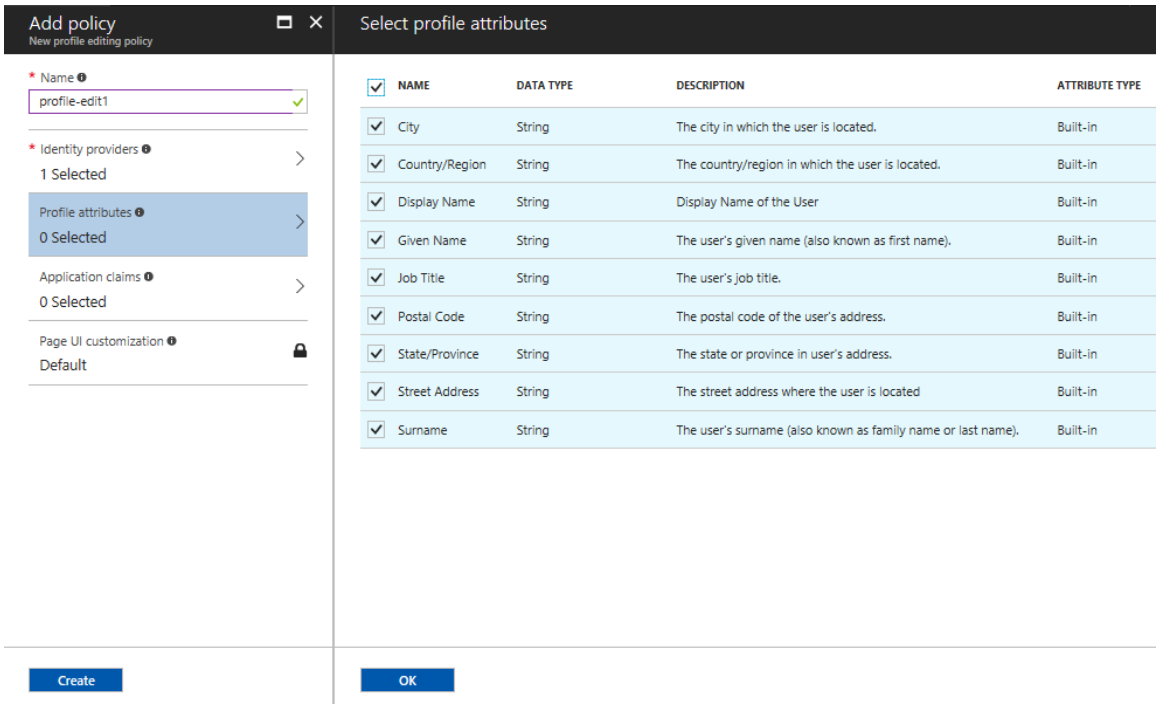
14. Click on **Profile editing policies**



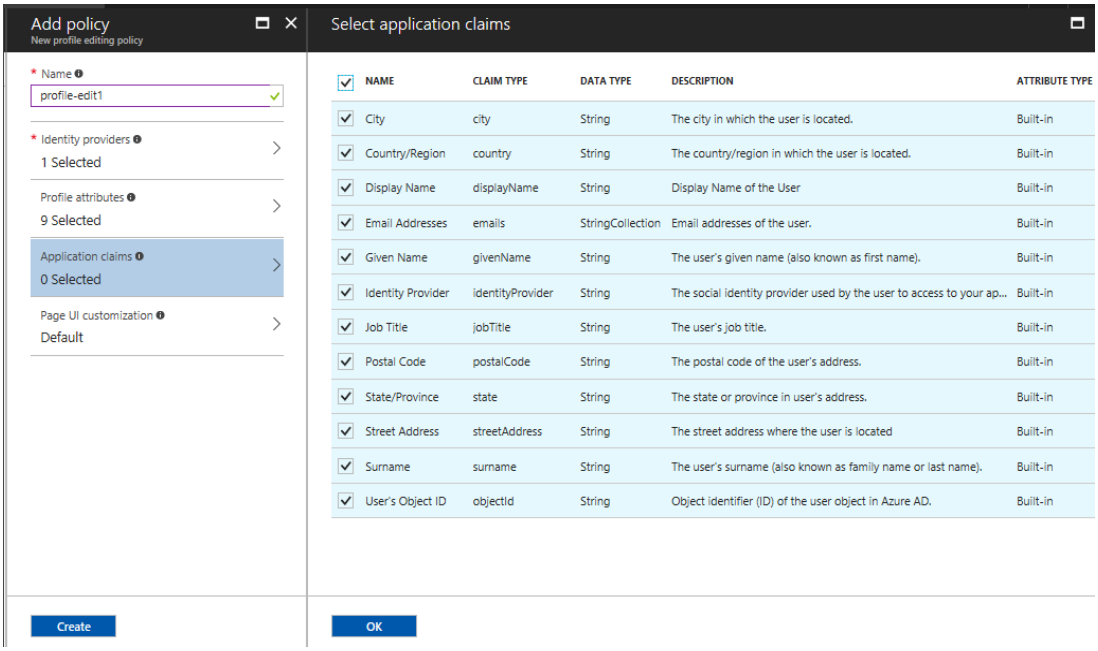
15. Provide a name and fill in the details as shown below.



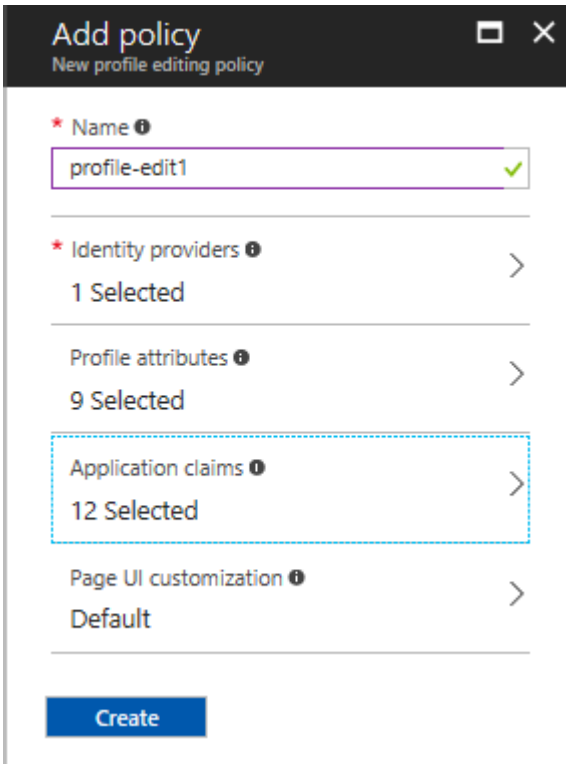
16. Select all the **Profile attributes** and click on **OK**.



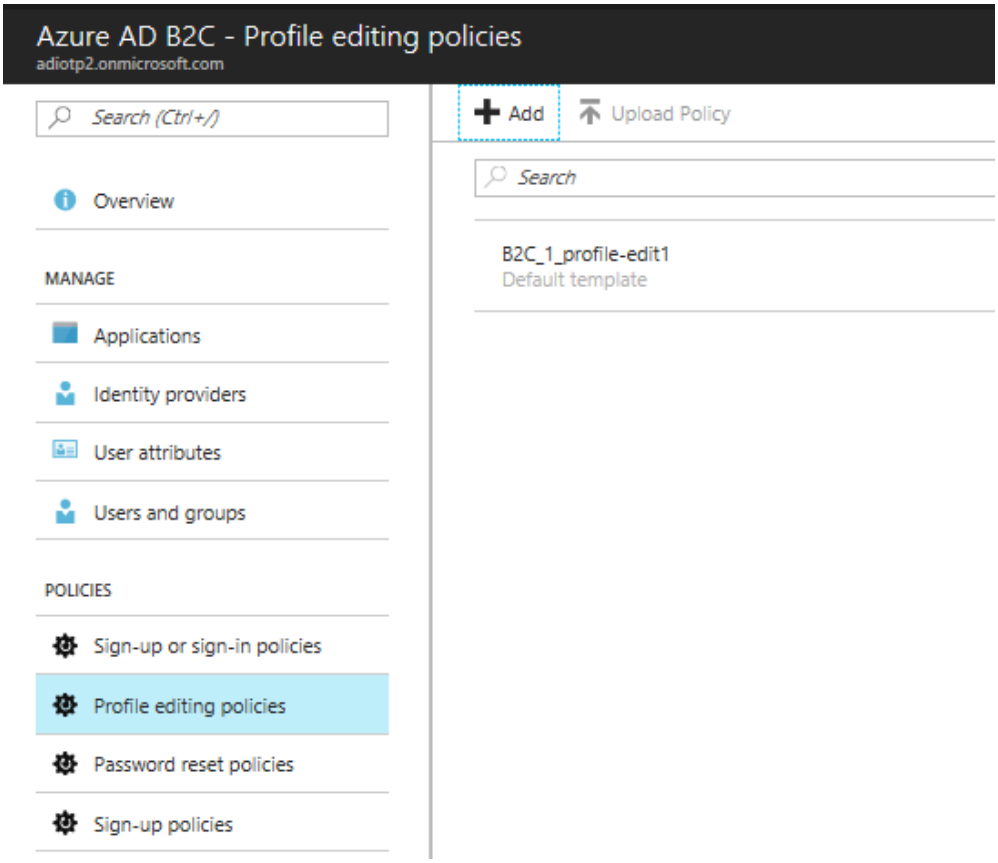
17. Select all the **Application claims** and then click on **OK**.



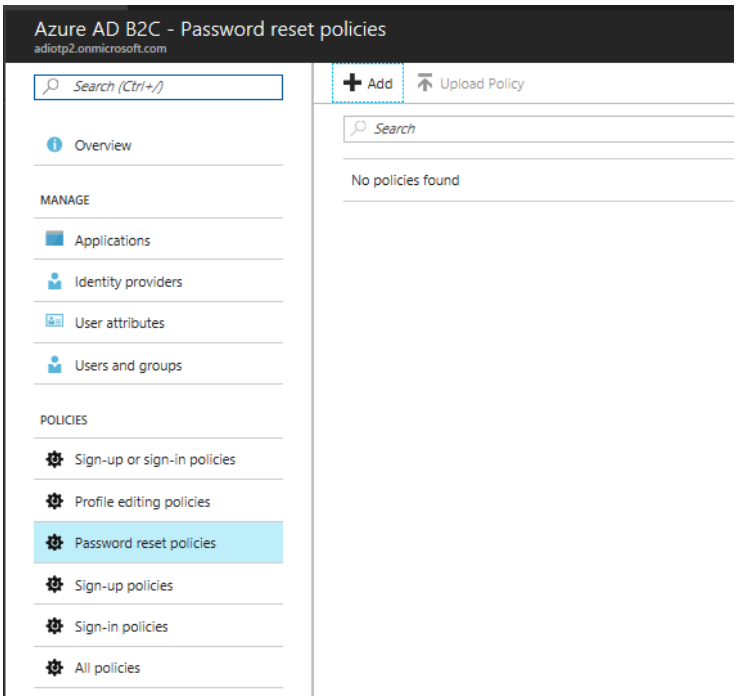
18. After filling in the details, click on **Create**.



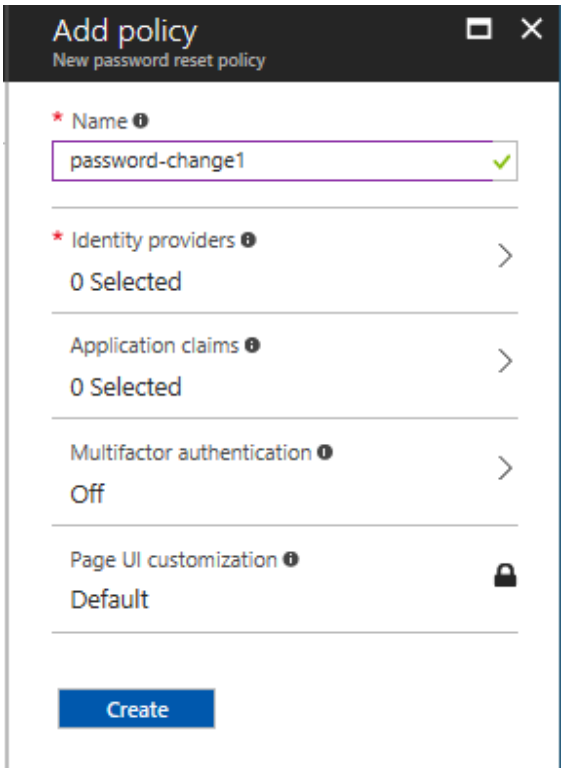
19. Once the deployment is completed, the below screen will appear.



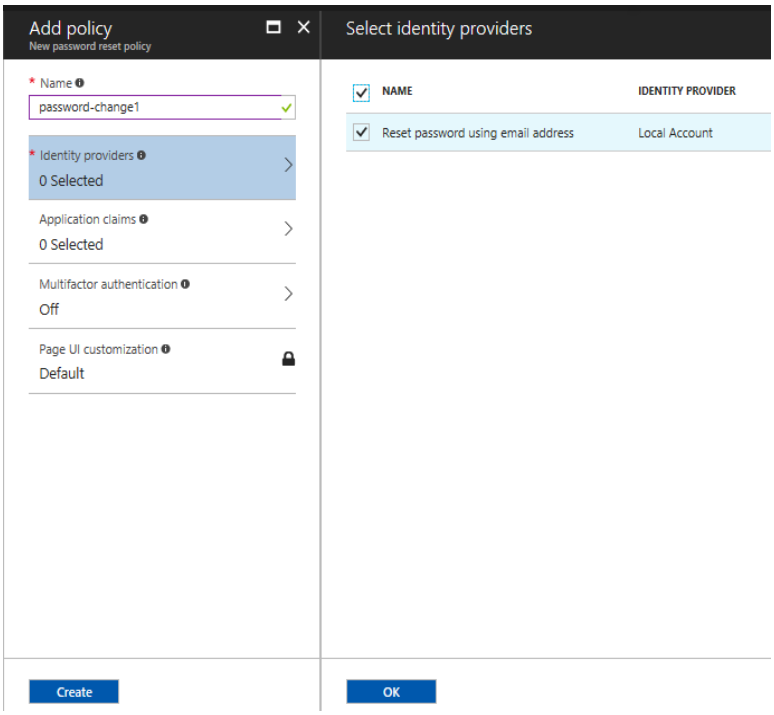
20. Click on **Password reset policies** and click on **Add**.



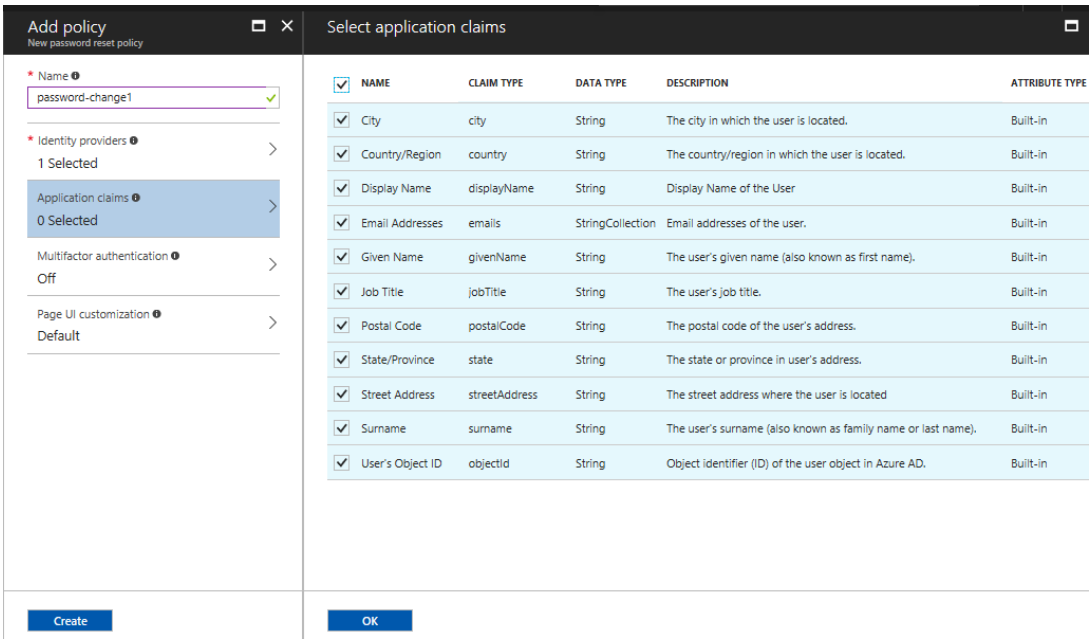
21. Provide the name of policy and fill the details as shown in the below screen.



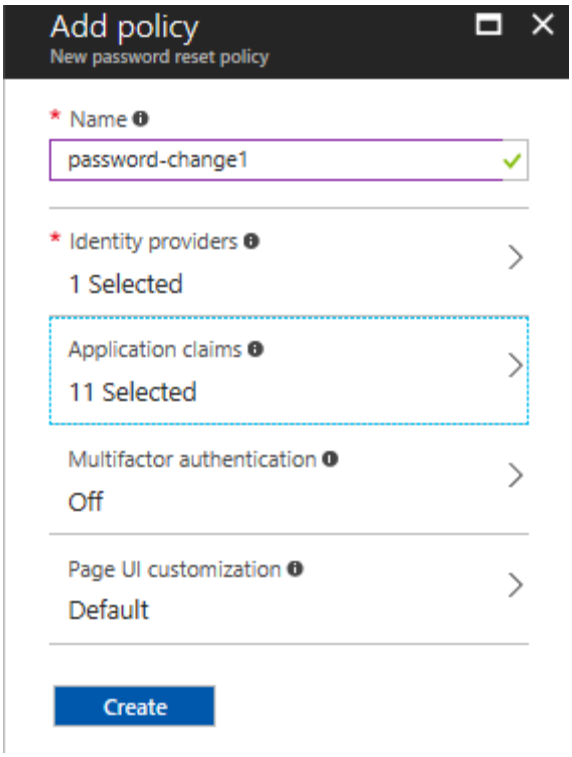
22. Check in **Reset password using email address** under **identity providers**.



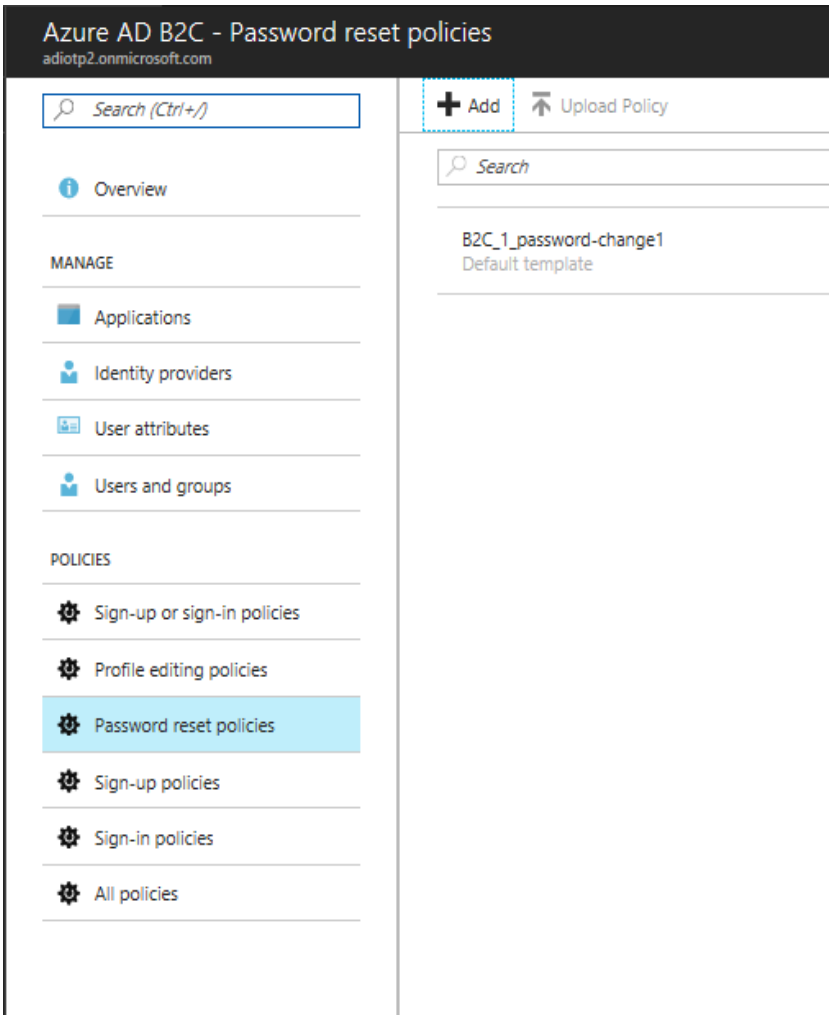
23. Select all **Application Claims** as shown below.



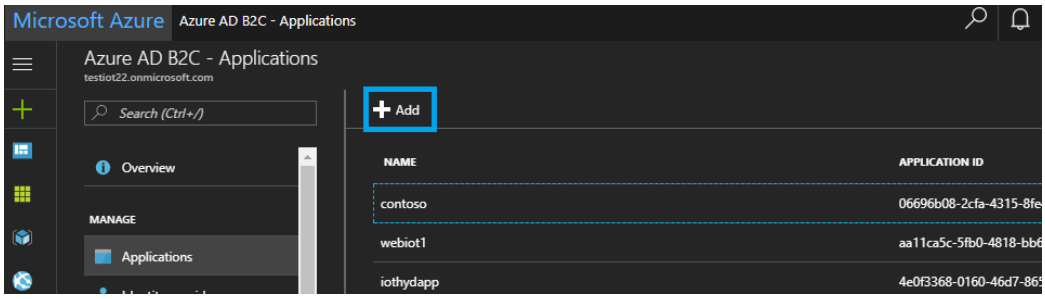
24. Click on **Create**.


Add policy
New password reset policy
* Name
password-change1
* Identity providers
1 Selected
Application claims
11 Selected
Multifactor authentication
Off
Page UI customization
Default
Create

25. Once the deployment is completed, the below screen will appear.



26. Click on the **Applications** tab and click **Add** to create a new application. Provide a name for the application.



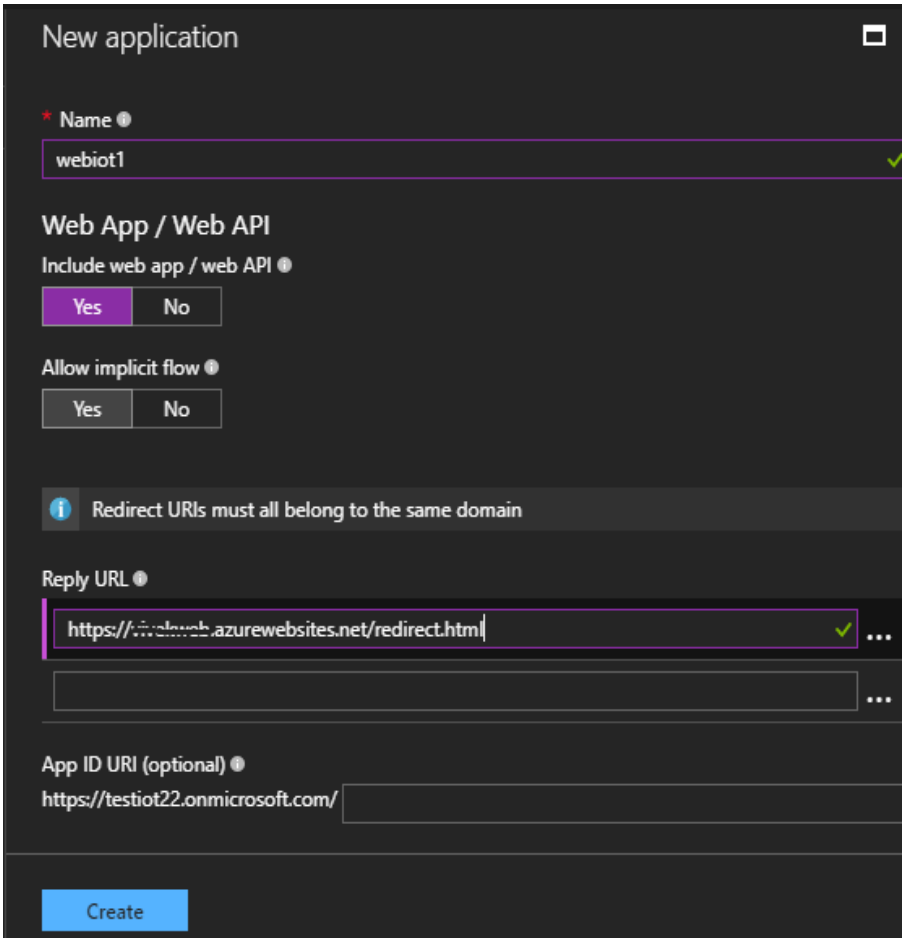
27. Under the Web APP/Web API tab, click on **Yes** to provide a redirect URL for your application. Add an entry in the Redirect URL section of the B2C application in the following format:

    https://<*name of the web app*>.azurewebsites.net/redirect.html

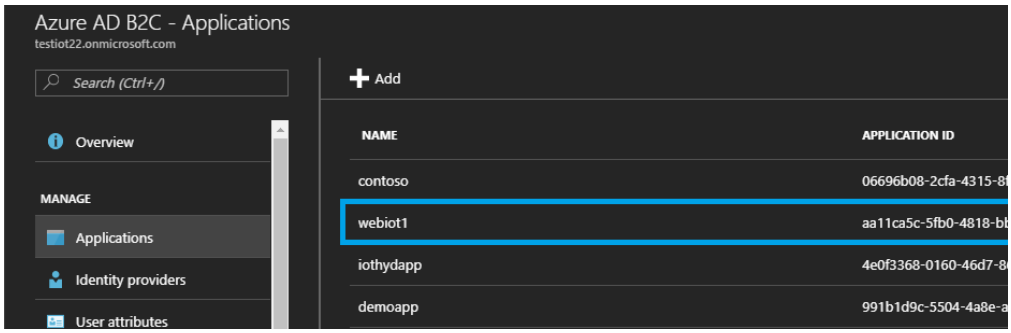
    During the web app registration with PowerBI, we will use this reply URL.
    Example: https://iotweb.azurewebsites.net/redirect.html

    After that, click on **Create**.

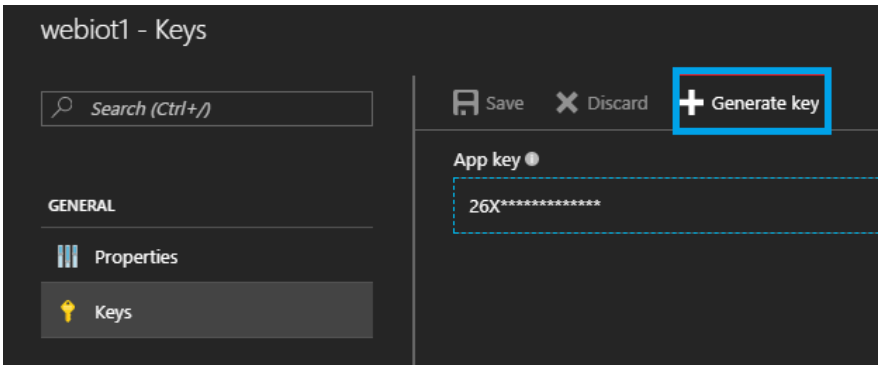
    This web app is used for authenticating the Energy management user login/ registration.



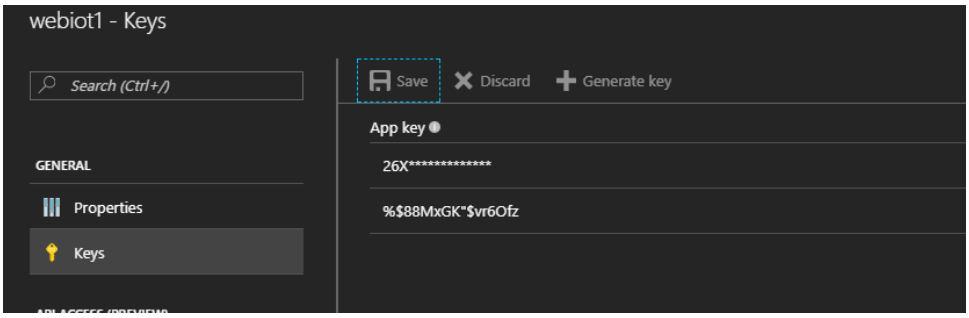
28. When you save that application, it will generate a unique application id and be used while deploying ARM template.



29. Select the application you created, then click on **Keys** > **Generate key** > **Save.**



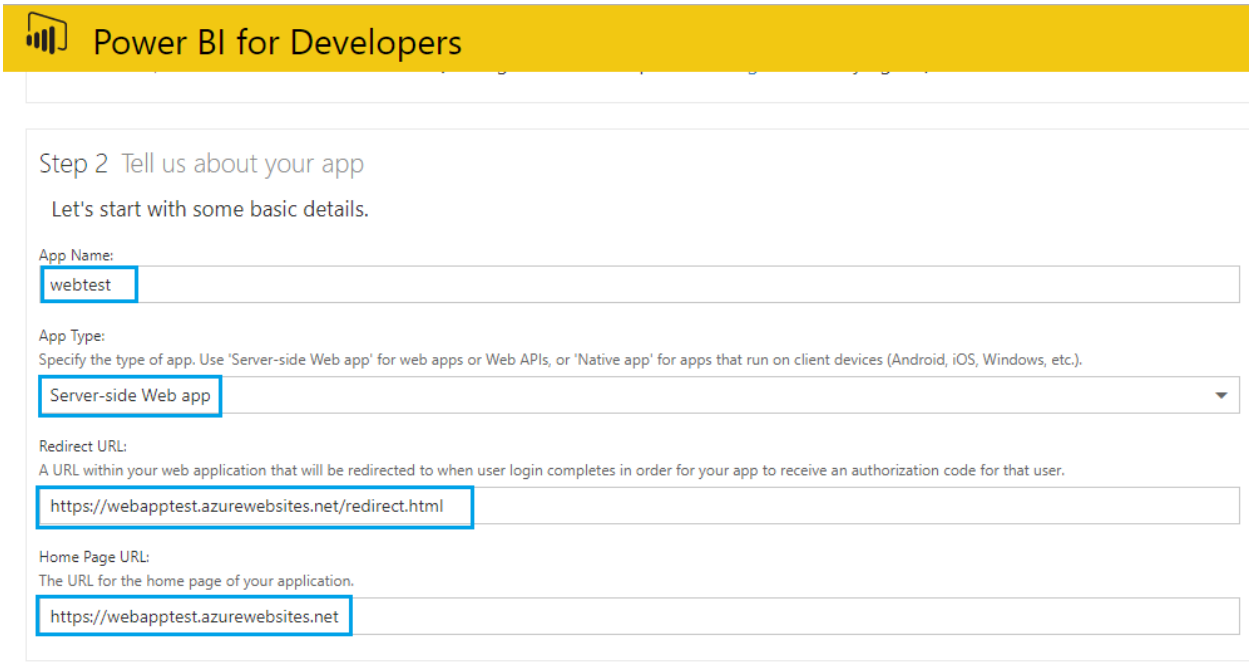
30. **Copy** the secret key.



4.3. Power BI Configuration

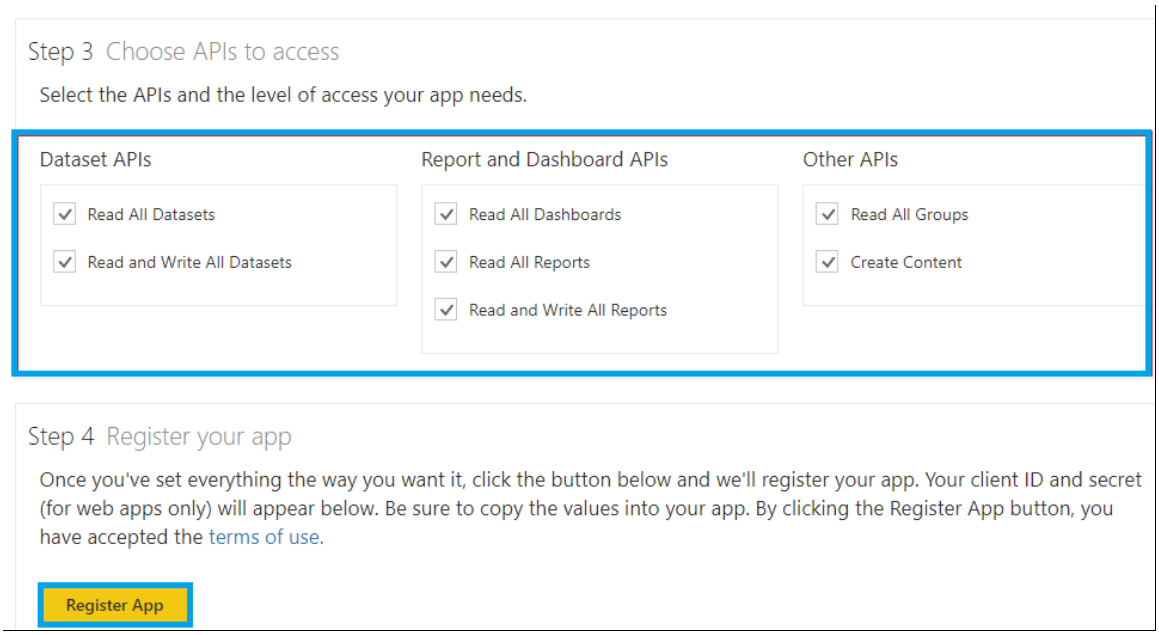
1. Go to https://dev.powerbi.com/apps and register the web app.
    a. Login to your Power BI account with the Azure Login credentials that have Global admin permissions.

b. Provide a name for your web app (This is different from what we created before).
c. Select App type "server-side Web App".
d. Enter the Redirected URL and Home URL, same as you gave in Azure AD B2C tenant URL without "/redirect.html" for Home URL.

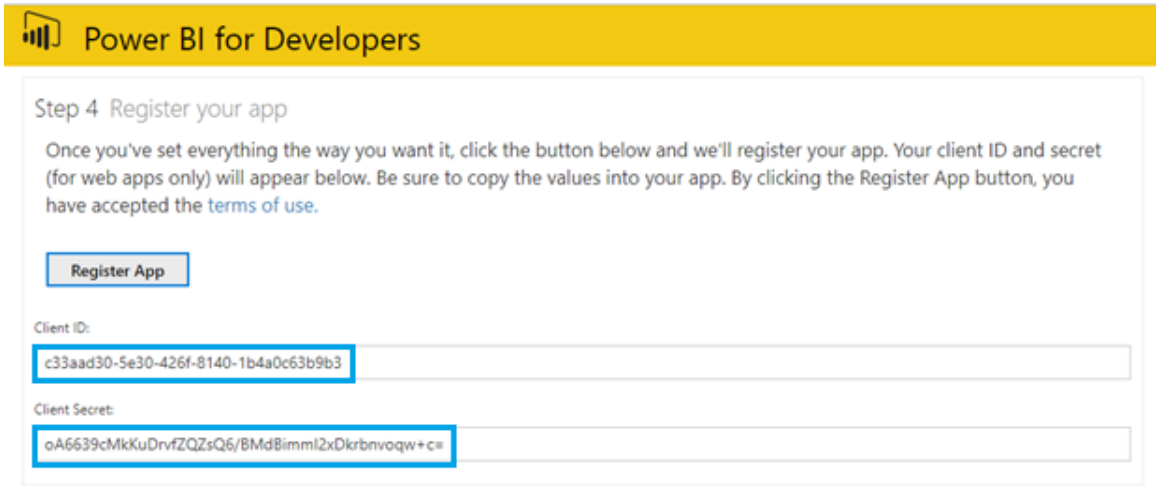


e. Select check boxes for required API's (select all check boxes for best practice).
   - Read all datasets
   - Read and write all data sets
   - Read all dashboards
   - Read all reports
   - Read and Write all reports
   - Read all Groups
   - Create content

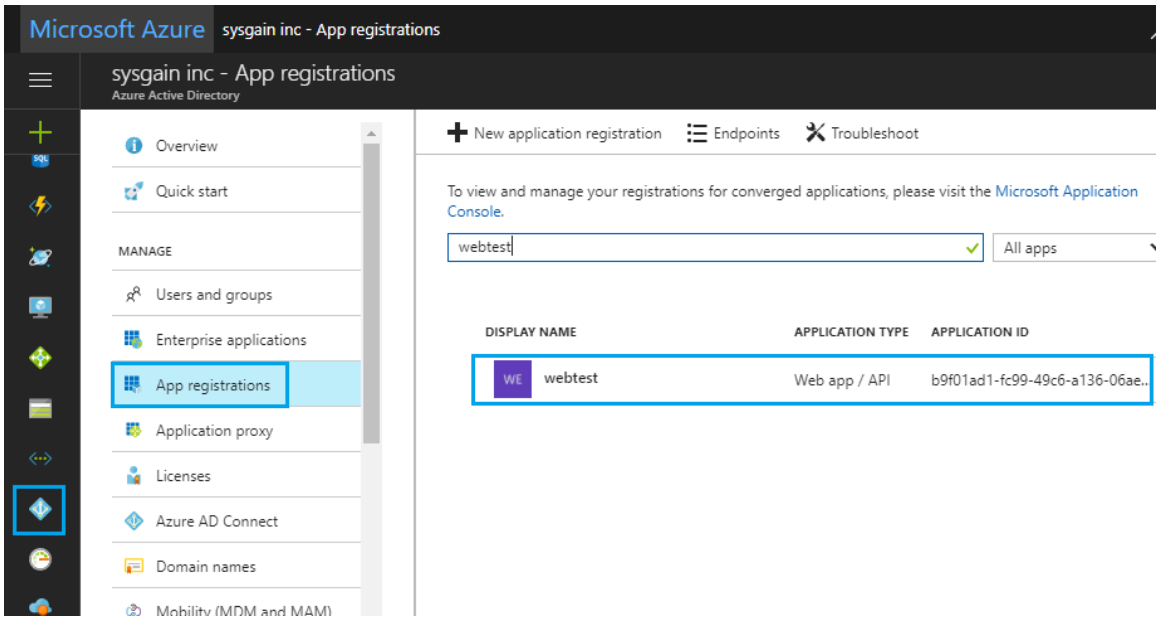
f. Click on Register App.



g. The Client id and secret key will be generated. Note down these keys locally, as you will use these later in the configuration.

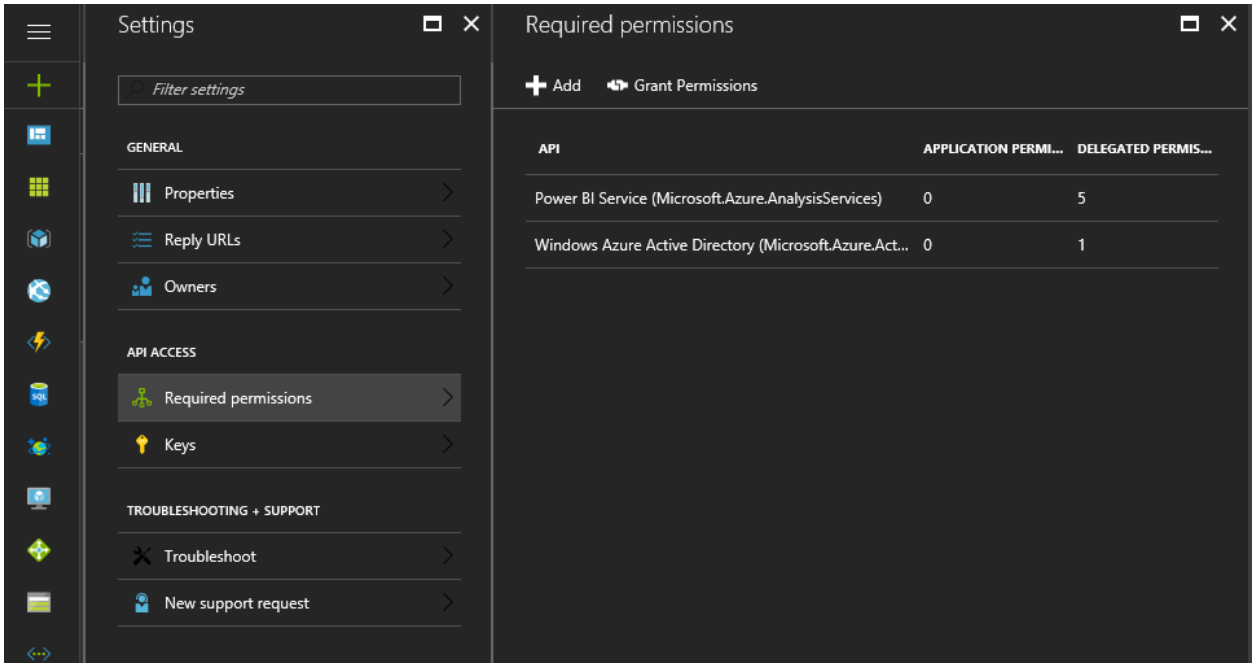


2. Go to Azure Active Directory from Your Azure Account and click on the **App registrations** tab. Select the app you just created from the list.



NOTE: To grant permissions to the app you must be a Global Administrator in the Tenant.

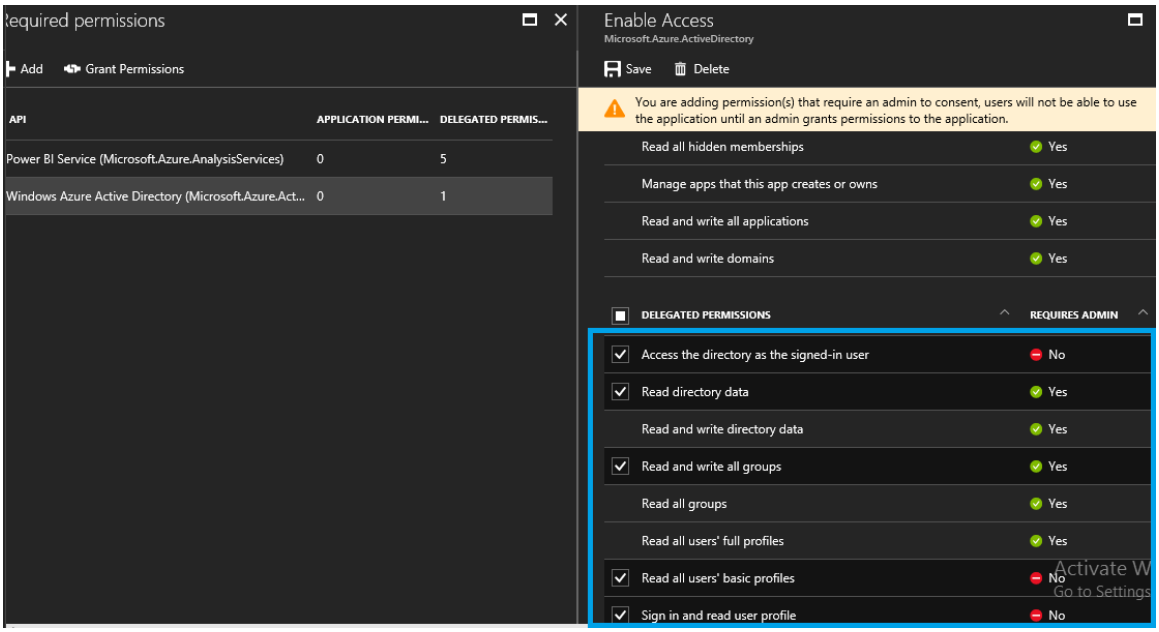
3. Click on the **app**, navigate to all settings, and give the required permissions.



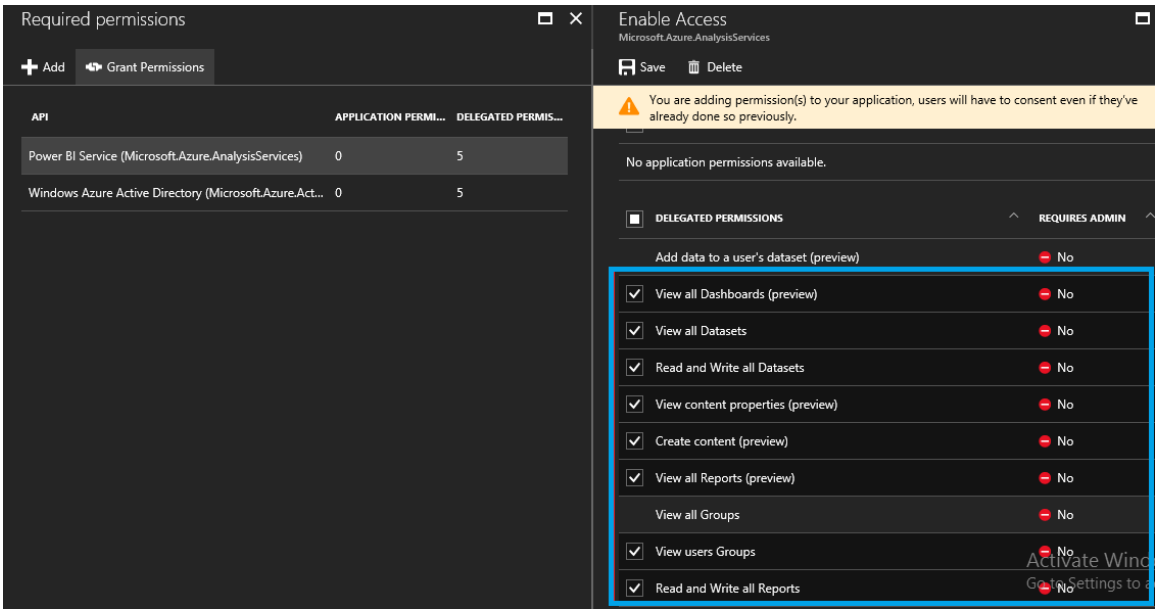
4. Enable the following access under delegated permissions in **Windows Azure Active Directory.**
    - Access the directory as the signed in users

- Read directory data
- Read and write all groups
- Read all user's basic profiles
- Sign in and read user profile

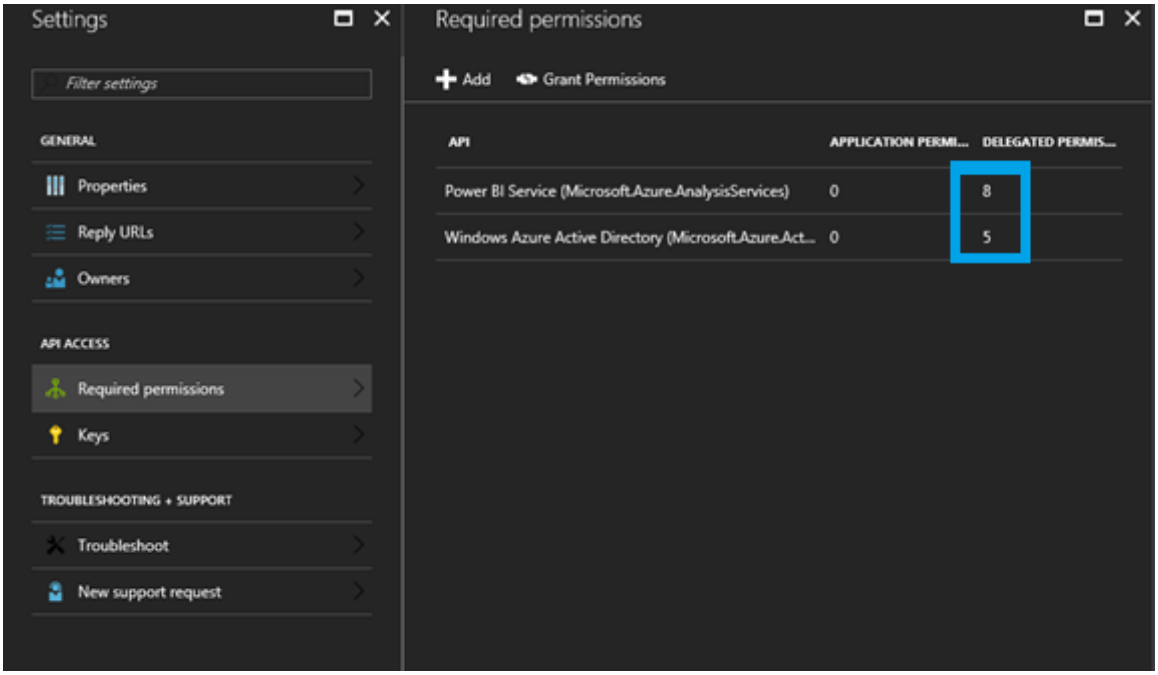
After that click on **Save.**



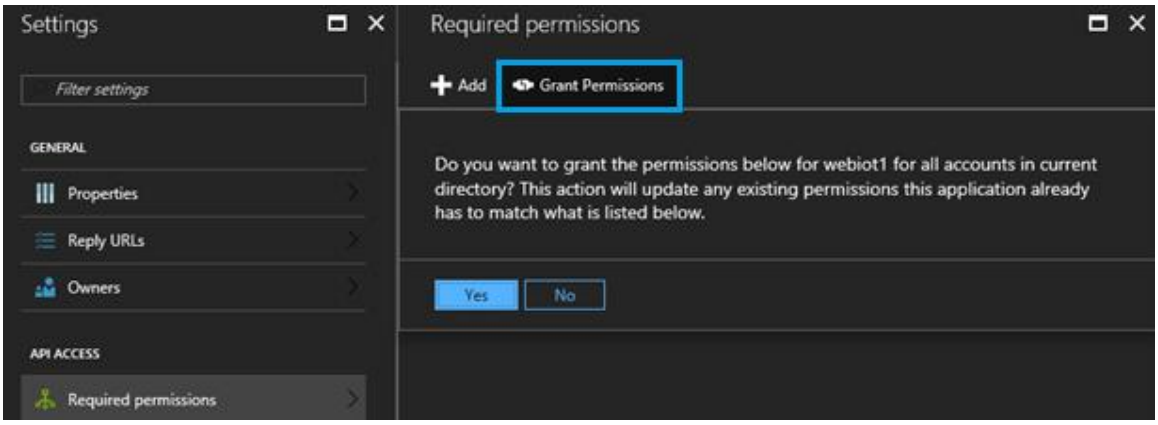
5. Enable the following access under delegated permissions in Power BI access.
    - View all datasets
    - View all dashboards
    - View content properties
    - View all reports
    - Create content
    - View user groups
    - Read and write all datasets
    - Read and write all reports



6. The user can see the number of permissions which have been added.



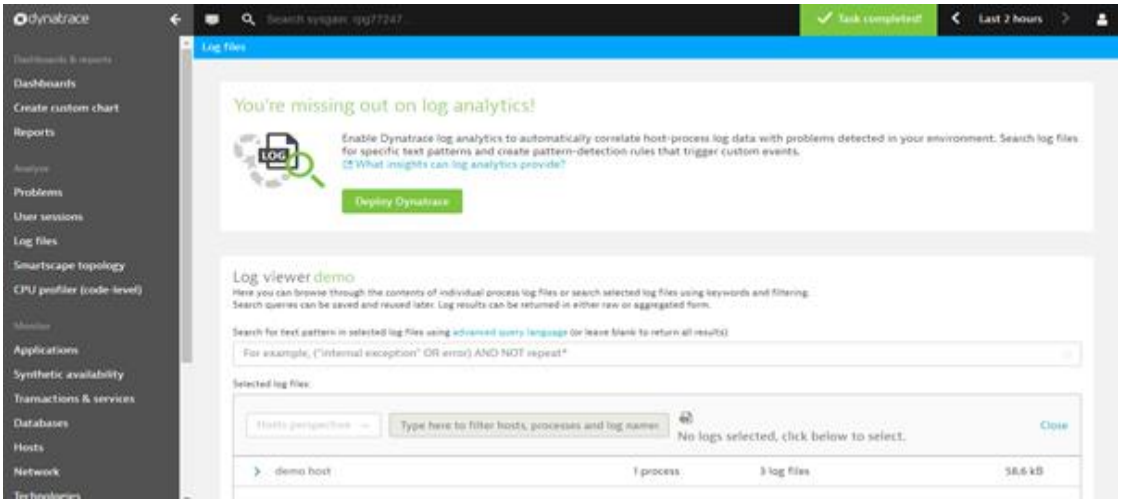
7. Click on **Grant Permissions**, then click **Yes**.



4.4. Dynatrace Account Creation (If You Don't Have an Existing Account)

Login to **Dynatrace SaaS** using URL: https://signin.dynatrace.com/

Existing Users: For users who already have a Dynatrace SaaS Account, login and navigate to **Log files** from the left side menu and click on "Deploy Dynatrace".



Please follow the process from "point 5" in the below section.

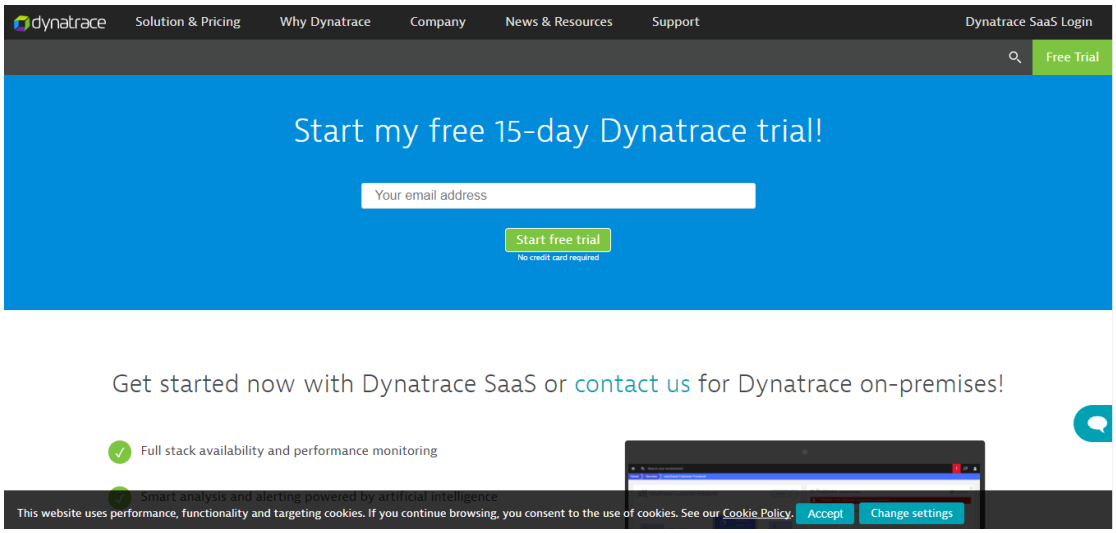
New Users: Please follow the below steps for "Sign up to Dynatrace trial SaaS for 15 days."

If you want to buy a license, please contact Dynatrace support.

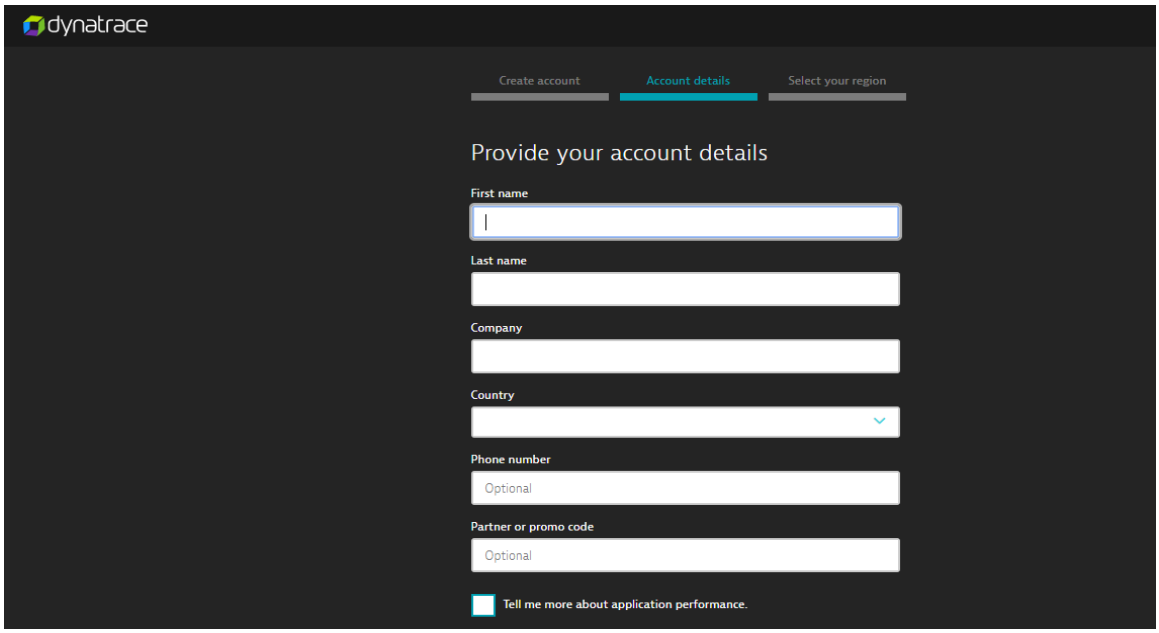
Support URL: https://www.dynatrace.com/support/

1. Sign up for a free trial on the Dynatrace home page by using an email address and click on **"Start Free Trial".**

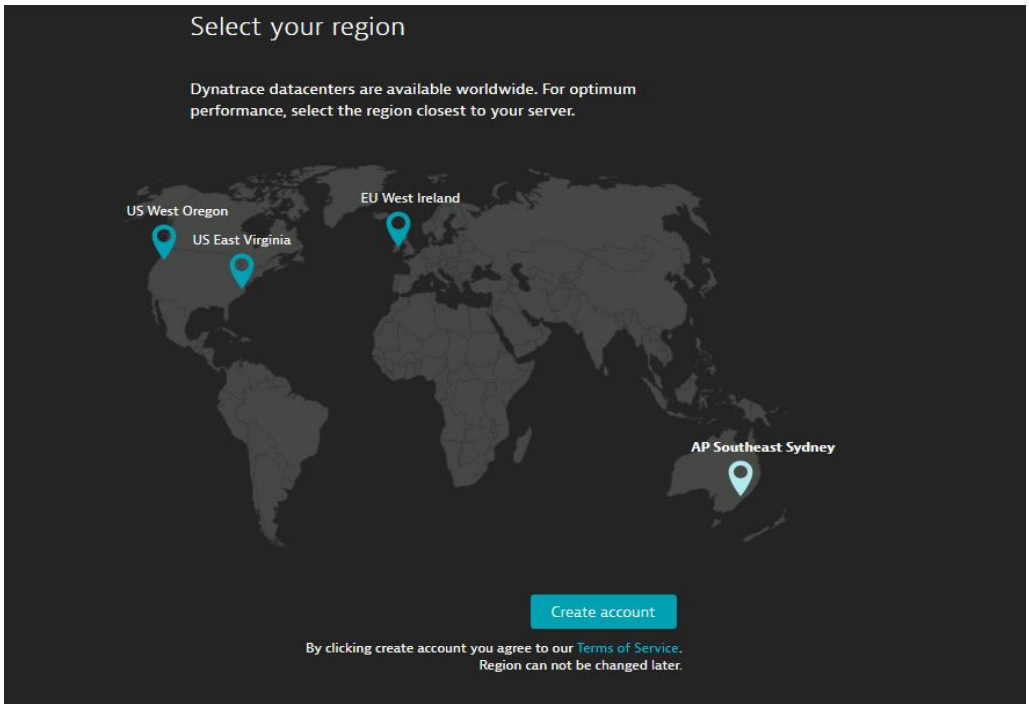
   Dynatrace home page - https://www.dynatrace.com



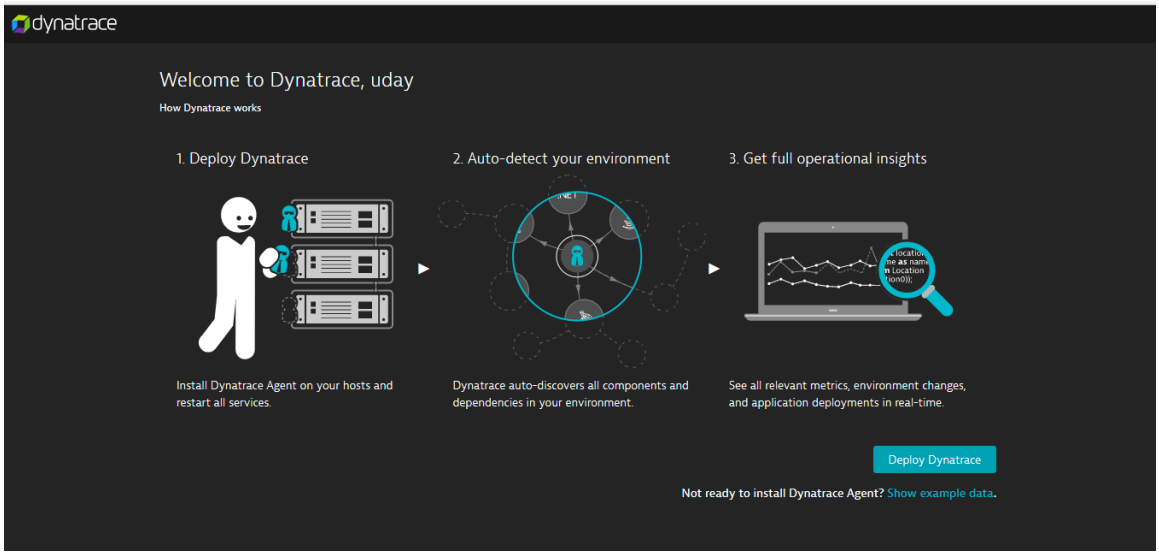
2. The below screen will appear. Fill out the **Create account, Account details** and **Select your region** screens.



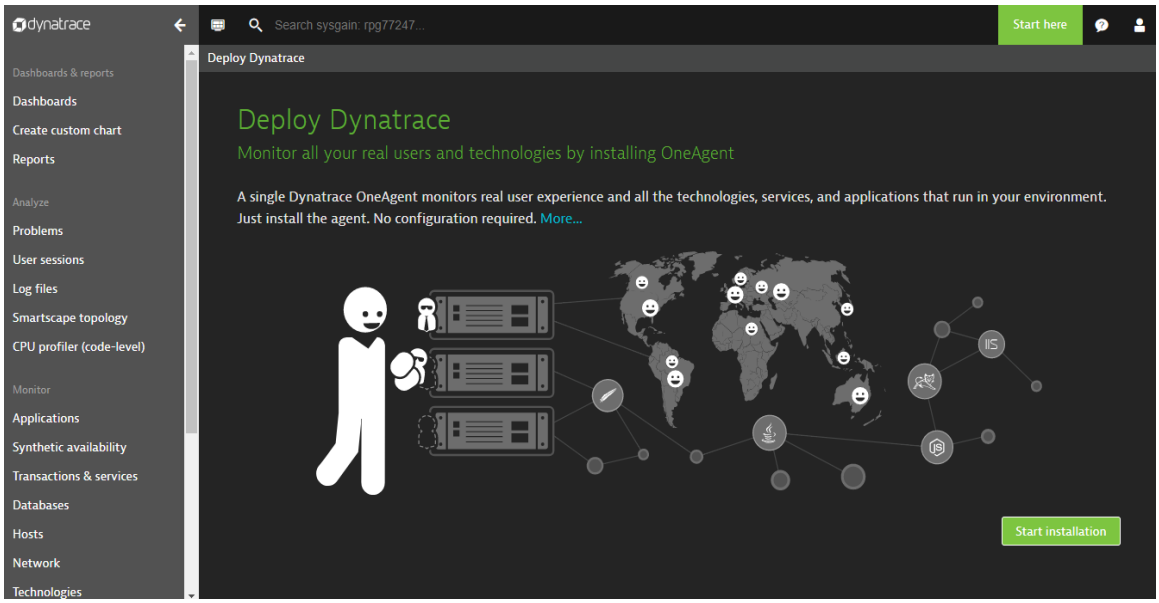
3. Select your region and click on **"Create account"**.



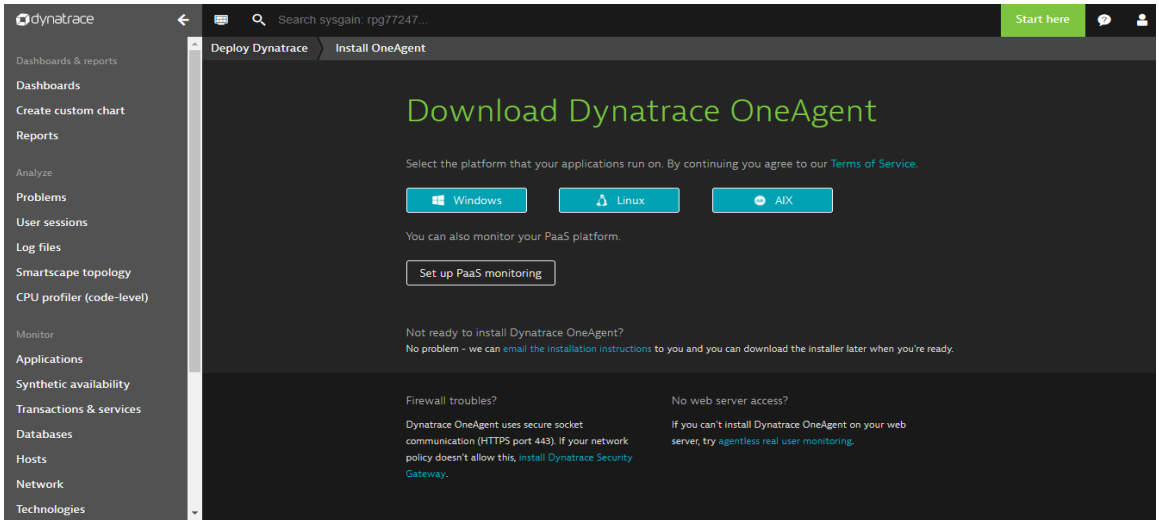
4. Click on **"Deploy Dynatrace".**



5. Click on **"Start installation".**

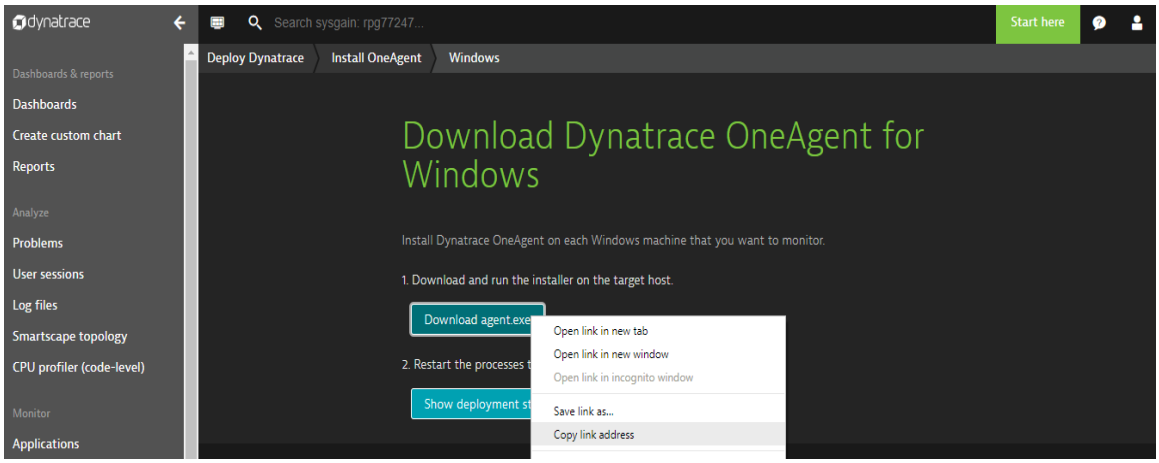


6. On the next screen, click "**Windows**".



7. From the below screen, Copy the link by right clicking on the **"Download agent.exe"**. Save the URL, which will be used while we configure Dynatrace.

   E.g. URL -
   https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix



5. Input Parameters

Parameter Name	Description	Allowed Values	Default Value
adminUsername	Username for all the Virtual Machines (for linux and Windows), make a note of the Username this will be used further	Any string	adminuser
adminPassword	Password for Windows Virtual Machines,make a note of the Password this will be used further	Password must be 12 characters and have 3 of the following 1 lower case character, 1 number, and 1 special character	
domainName	The FQDN of the Active Directory Domain to be created	Any domain names. (E.g. msfiot.com)	
bastionVMSize	Bastion Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
chefWorkstationVMSize	chef workstation Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2

adServerVMSize	Active directory Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
trendVMSize	trend Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
splunkVMSize	splunk Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
chefAutomateVMSize	chef Automate Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
PIAFDASQLServerVMSize	PIAFDASQL Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
PIBAServerVMSize	PIBA Virtual Machine size	Select the instance type from dropdown menu	Standard_DS2_v2
websiteName	Give the websitename used in the reditect URL during the webapplication creation (E.g : give 'iotwebsite' from https://iotwebsite.azurewebsites.net/redirect.html	FQDN prefix for the application endpoint. Should be unique	
sqlAdministratorLogin	The SQL authentication admin user of the SQL Server, make a note of Username this will be used further	Any string	sqluser
sqlAdministratorLoginPassword	The SQL authentication password of the admin user of the SQL Server, make a note of the Password this will be used further	Password must be 12 characters and have 3 of the following 1 lower case character, 1 number, and 1 special character	
skuName	Describes plan's pricing tier and instance size. Check details at https://azure.microsoft.com/en-us/pricing/details/app-service/	D1, B1, B2, B3, S1, S2, S3, P1, P2, P3, P4	S1
skuCapacity	Describes plan's instance count	minValue – 1 maxValue - 4	1
emailHost	Describes the host name for sending email notifications	Any string	

senderEmail	Describes the email ID of the sender for email notifications.	Email format. (E.g. iot@microsoft.com)	
senderEmailPassword	Describes the password for the sender email ID for email notifications.	Valid password string	
b2cTenant	Azure Active Directory B2C is a cloud identity service allowing you to connect to any customer. Describes B2C tenant name directory.	Valid B2C tenant. (E.g. iot.onmicrosoft.com)	
b2cClientId	Describes the client Id of the application registered in B2C directory.	GUID	
b2cClientSecret	Describes the Client secret of the application registered in B2C directory.		
b2cSignUpPolicyId	Sign-up policy allows you to control behaviors by configuring the Account types and Attributes. This field is the id for the B2C Sign up policy	Valid B2C sign up policy. (E.g. B2C_1_suppolicy2)	
b2cSignInPolicyId	Describes the B2C Sign in policy	Valid B2C sign in policy. (E.g. B2C_1_sinpolicy2)	
b2cEditProfilePolicyId	Describes the B2C Profile Editing policy.	Valid B2C Profile Editing policy. (E.g. B2C_1_peditpolicy2)	
b2cChangePasswordPolicy	Describes the B2C Change Password policy.	Valid B2C Change Password policy. (E.g. B2C_1_cpasspolicy)	
MLskuName	Pricing tier for machine learning workspace.	S1, S2, S3	S1
chefUserFirstName	First name of the Chef user.	Any string	
chefUserLastName	Last name of the Chef user.	Any string	
chefuserEmail	Email of the Chef user.	Valid email address (E.g. orguser@noone.com)	
chefOrgShortname	Short name of the Chef's organization	Any string	

6. Azure Resource Manager Template Deployment

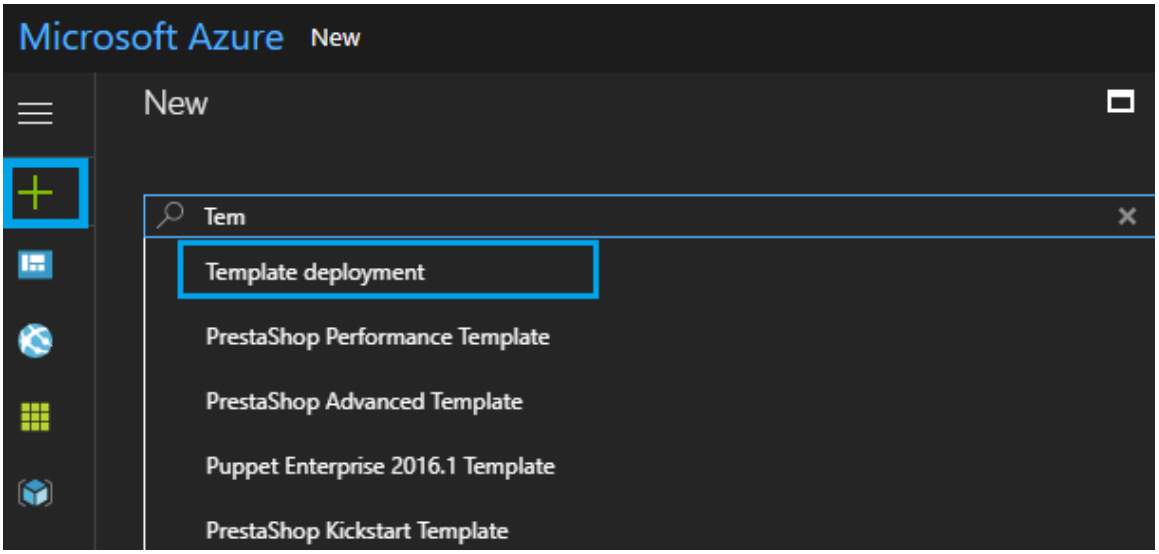
Click on below Git hub repo url

https://github.com/sysgain/iot-automation/tree/sysgainiot

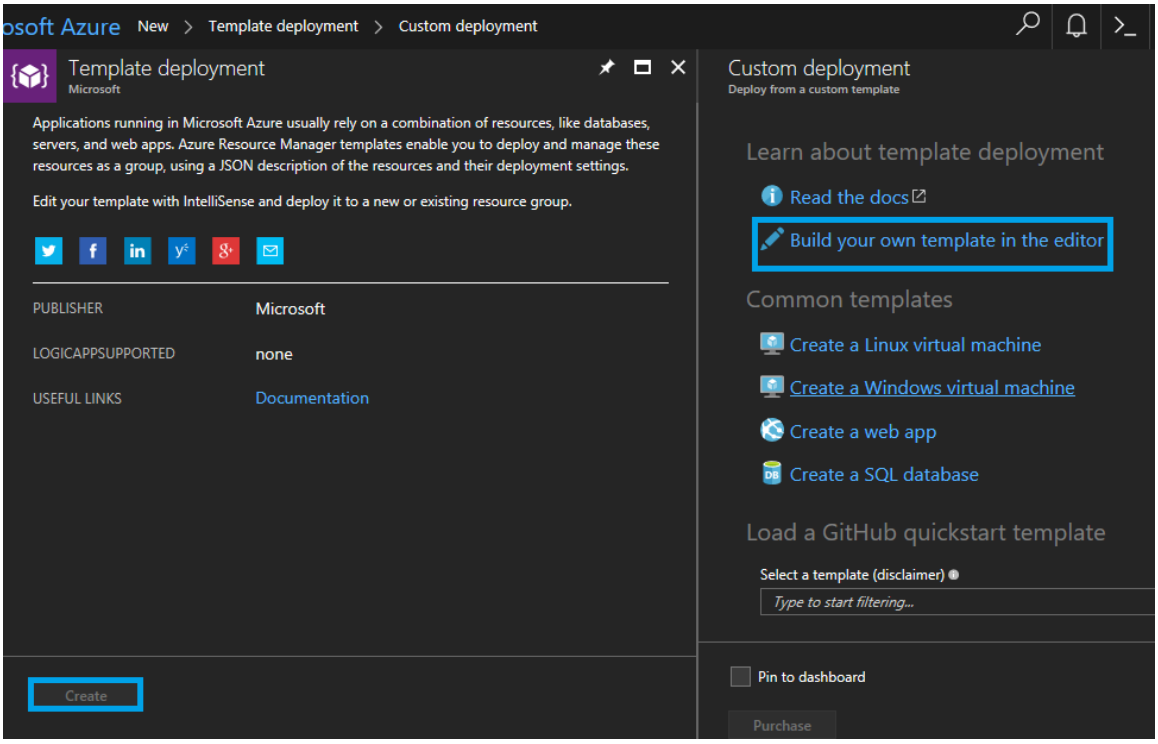
Take the main-template.json raw

Note: Make sure to deploy fortigate-main-template.json and main-template.json in same resource group.

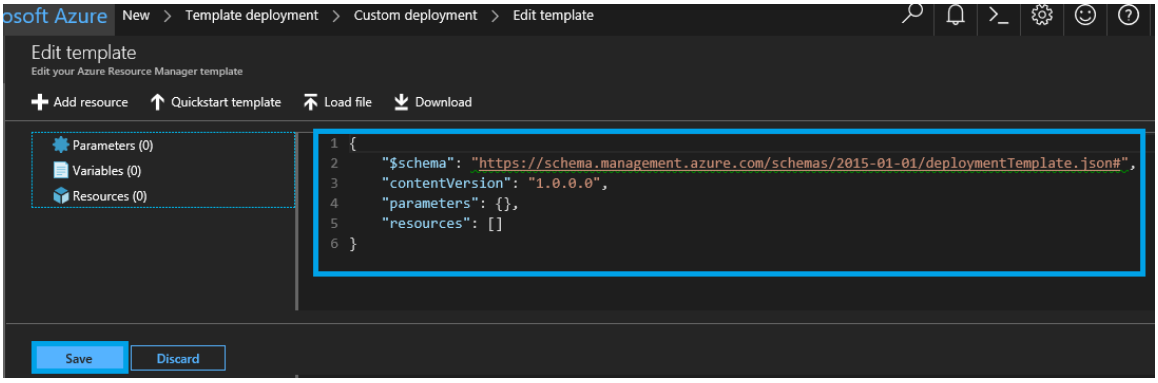
1. Open Azure portal, Navigate to **New (+)**, search for **Template deployment**.



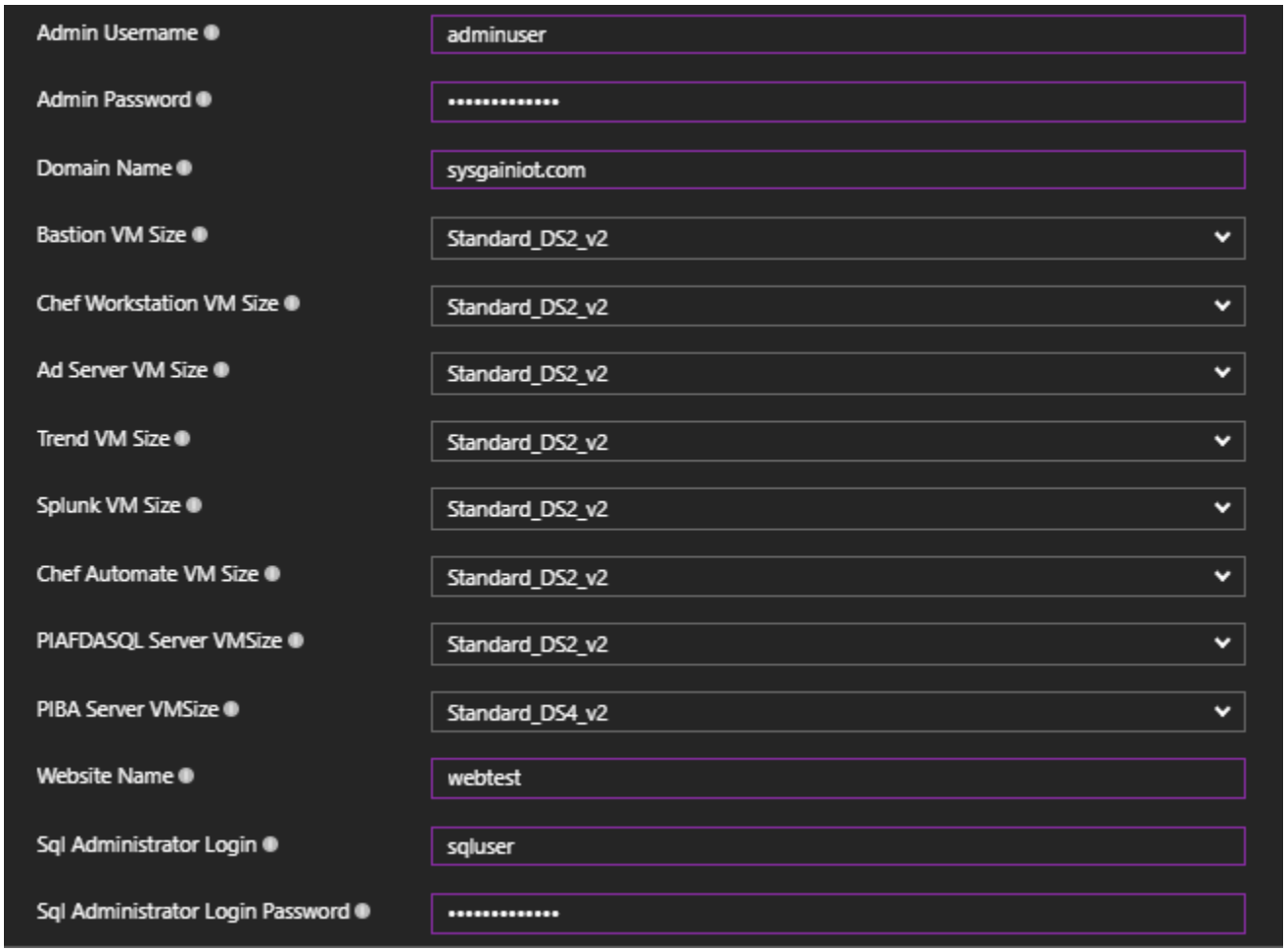
2. Click on **create** and click on **Build your own Template**.

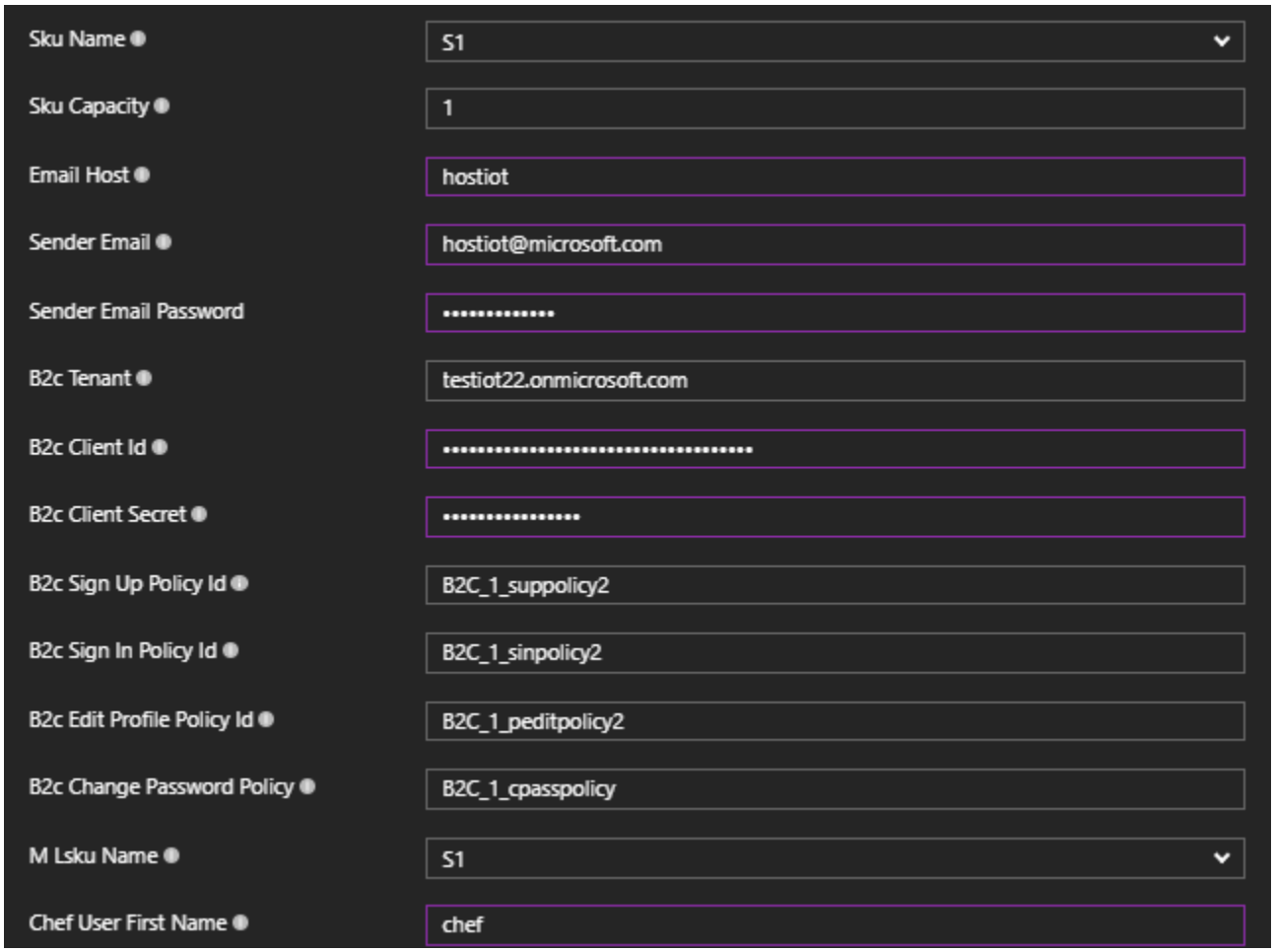


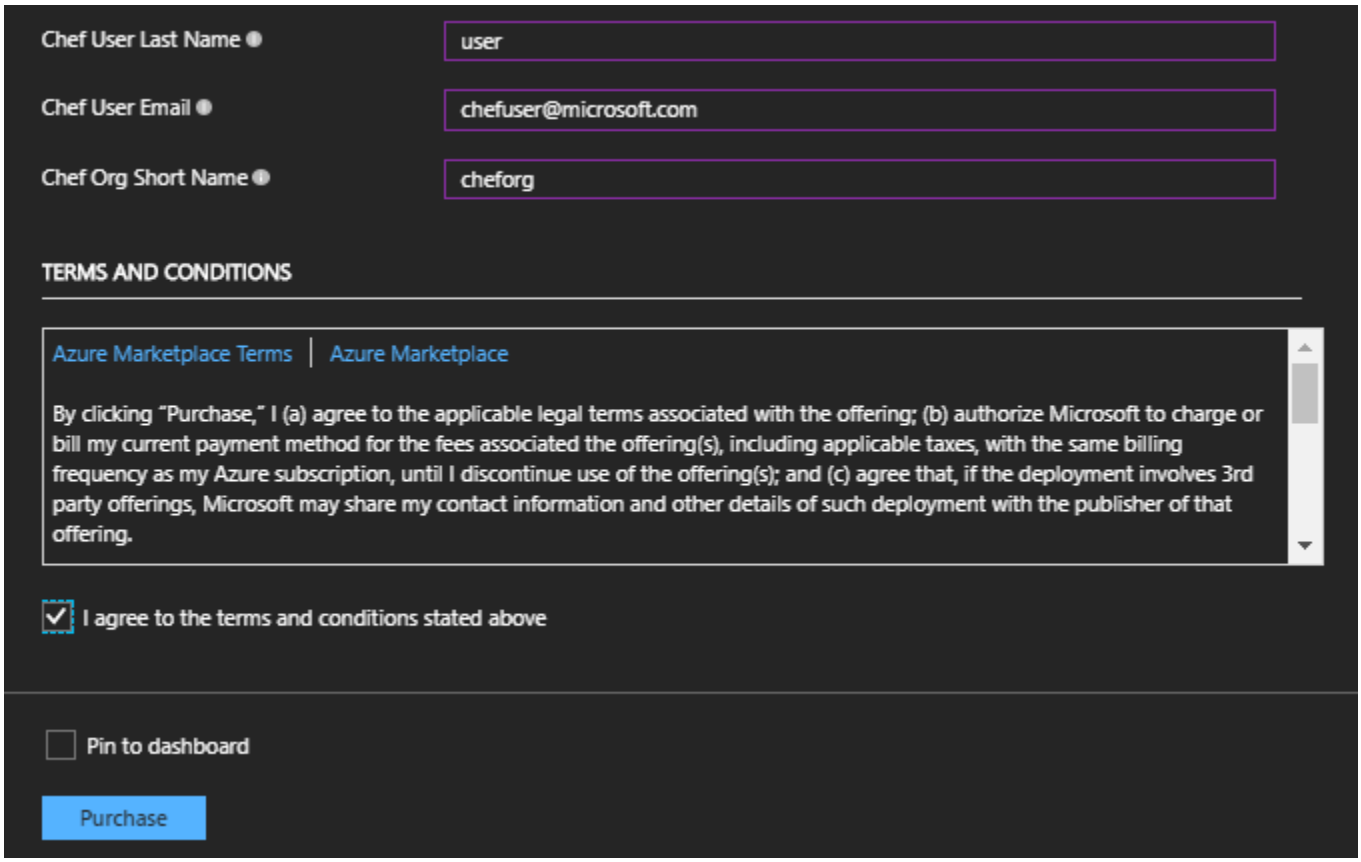
3. Replace the template and click on **Save**.



4. From Azure Portal, deploy the template by providing the following parameters in custom deployment settings


Admin Username
adminuser
Admin Password
Domain Name
sysgainiot.com
Bastion VM Size
Standard_DS2_v2
Chef Workstation VM Size
Standard_DS2_v2
Ad Server VM Size
Standard_DS2_v2
Trend VM Size
Standard_DS2_v2
Splunk VM Size
Standard_DS2_v2
Chef Automate VM Size
Standard_DS2_v2
PIAFDASQL Server VMSize
Standard_DS2_v2
PIBA Server VMSize
Standard_DS4_v2
Website Name
webtest
Sql Administrator Login
sqluser
Sql Administrator Login Password

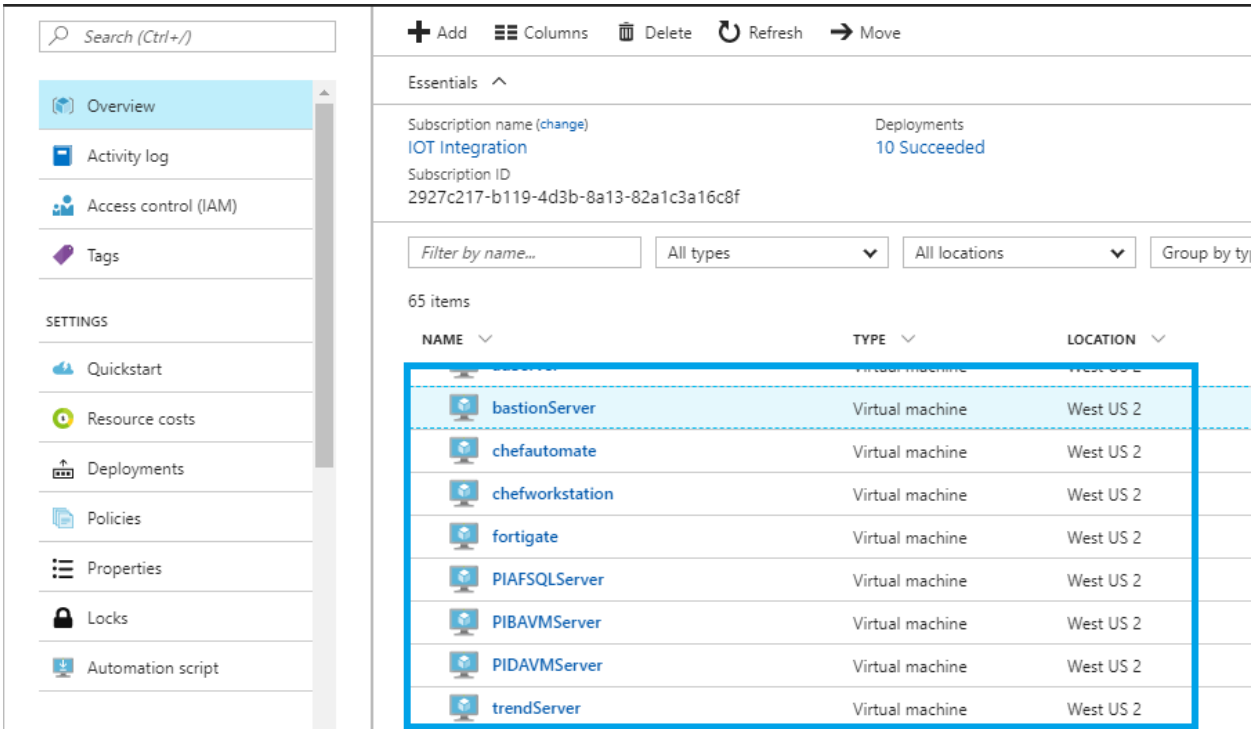

Sku Name
S1
Sku Capacity
1
Email Host
hostiot
Sender Email
hostiot@microsoft.com
Sender Email Password
B2c Tenant
testiot22.onmicrosoft.com
B2c Client Id
B2c Client Secret
B2c Sign Up Policy Id
B2C_1_suppolicy2
B2c Sign In Policy Id
B2C_1_sinpolicy2
B2c Edit Profile Policy Id
B2C_1_peditpolicy2
B2c Change Password Policy
B2C_1_cpasspolicy
M Lsku Name
S1
Chef User First Name
chef



5. Once all the parameters are entered click on the terms and conditions check box click on **Purchase**.
6. After launching the template, the following resources will be created in a Resource Group:

- 2 App Services
- 1 App service plan
- 1 work space plan and work space in Machine Learning
- 8 Network interfaces
- 8 network security groups
- 3 public IP address
- 1 scheduler job collection
- 2 SQL databases
- 2 SQL Servers
- 8 storage accounts
- 8 disks
- 8 virtual machines
- 1 Virtual network

7. Below is the list of virtual machines that will be created in the Resource Group.

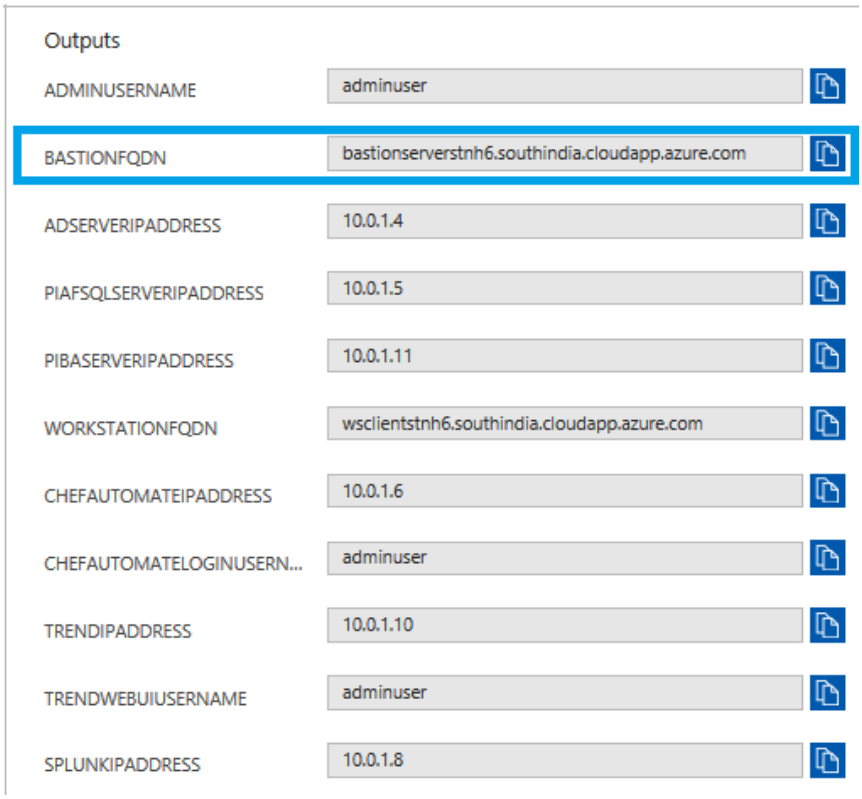


6.1. Output Parameters

Parameter Name	Description
Admin Username (adminUsername)	User name to log into any virtual machine in the deployment
Bastion FQDN (bastionFQDN)	FQDN of Bastion server
AD Server IP Address (adServerIPAddress	IP address to login to AD server
PI AF SQL Server IP Address (piafSQLServerIPAddress)	IP address of PI AF, PI DA and PI SQL server
PI BA Server IP Address (pibaServerIPAddress)	IP address of PI BA server
Workstation FQDN (workstationFQDN)	FQDN of Chef workstation. Used for creating cookbooks and uploading them to Chef server (Chef Automate)
Chef Automate IP Address (chefAutomateIPAddress)	IP address Chef Automate

Chef Automate login user name (chefAutomateLoginUsername)	Login username for Chef Automate
Trend DSM IP Address (trendIPAddress)	IP Address of Trend DSM
Trend Web UI Username (trendWebUIUsername)	Trend Username to login to DSM portal
Splunk IP Address (splunkIPAddress)	IP Address of Splunk
Splunk Web UI Username (splunkWebUIUsername)	Username to login to Splunk portal
FortiGate FQDN (fortigateFQDN)	FQDN of FortiGate VM
Azure SQL End Point (azureSQLEndpoint)	Used for data service setup
Azure SQL DB name (azureSQLDBName)	Used for data service setup
Azure SQL Username (azureSQLUsername)	Username to login to Azure SQL
Windows SQL Username (windowsSQLUsername)	Username to login to Windows SQL server
Web job Storage account name (webjobStorageaccntName)	Web job storage account
Website URL (websiteUrl)	We application URL

The below values of the output parameters are further used as credentials & to login to the Virtual Machines.



SPLUNKWEBUIUSERNAME	admin
FORTIGATEFQDN	fortigatestnh6
AZURESQLENDPOINT	sqlserverstnh6.database.windows.net
AZURESQLDBNAME	azuredb
AZURESQLUSERNAME	sqluser
WINDOWSSQLUSERNAME	sqluser
WEBJOBSTORAGEACCNTNAME	webjobstrstnh6
WEBSITEURL	https://mshydapp.azurewebsites.net/

7. Security and Monitoring Components

Bastion Host: The Bastion Host has the public IP address which is used to access the private instances as shown in the architecture diagram.

Dynatrace: Dynatrace provides unique operational insights with just one tool. It leverages full stack monitoring from the front-end, to the back-end, to infrastructure, to the cloud. It also helps to understand how application performance impacts your customers.

Chef Automate: Chef is a configuration management tool. That means it ensures that the expected files and software are present, configured correctly, and working as intended. We can use Chef for one server or thousands of servers to fulfill our requirements. It solves these things by treating infrastructure as a code.

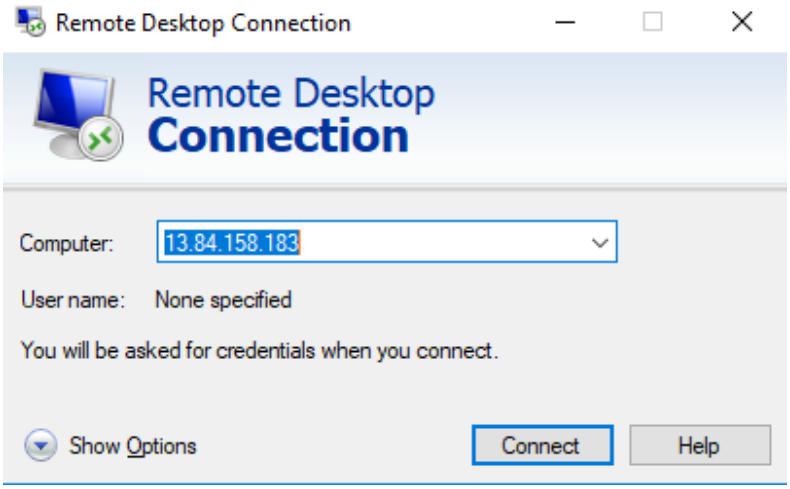
Trend Micro Deep Security Manager (DSM): This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents. The DSM is controlled using the web-based management console. Using the console, the administrator can define security policies, manage deployed agents, query status of various managed instances, etc. The integration with Splunk is done using this interface: no additional component or software is required.

Trend Micro Deep Security Agent (DSA): This component provides all protection functionality. The nature of protection depends on the rules and security settings that each DSA receives from the Deep Security Manager.

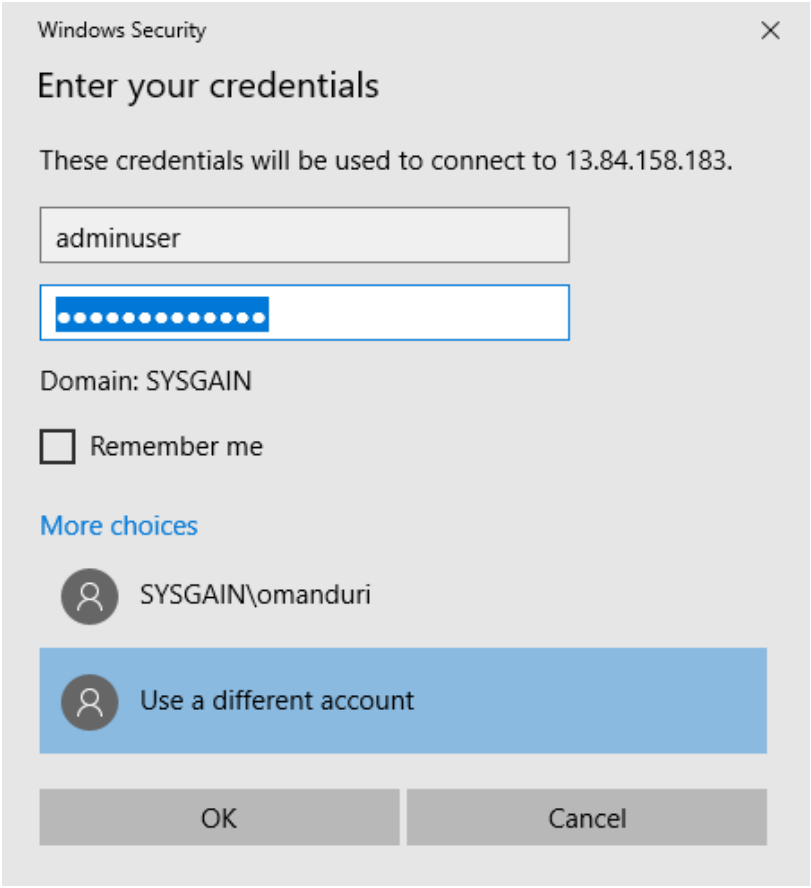
Splunk Enterprise: Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device.

7.1. Dynatrace

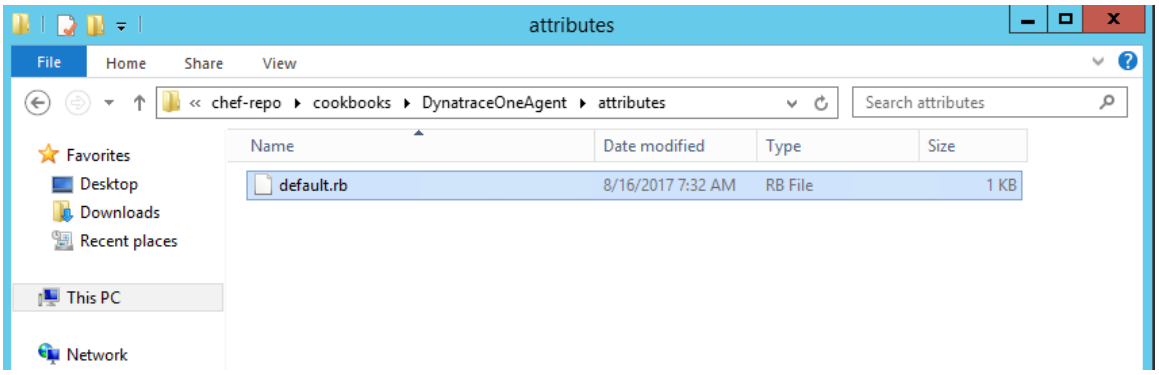
1. Log in to the **Chef Workstation** using the workstationFQDN provided in the output section.



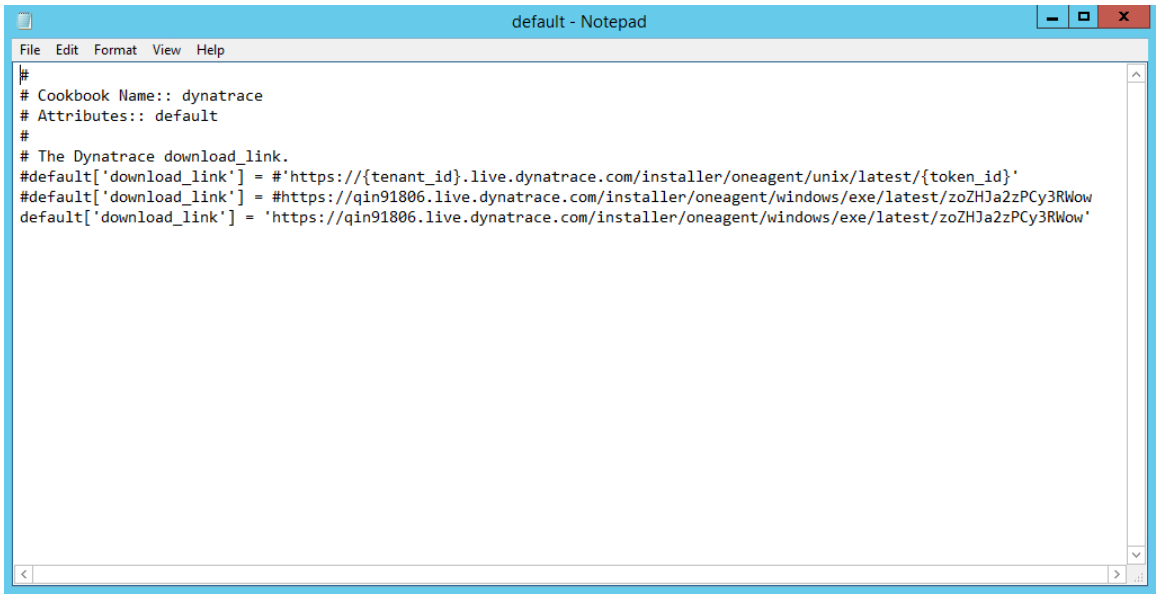
2. Enter the credentials provided in the output section.

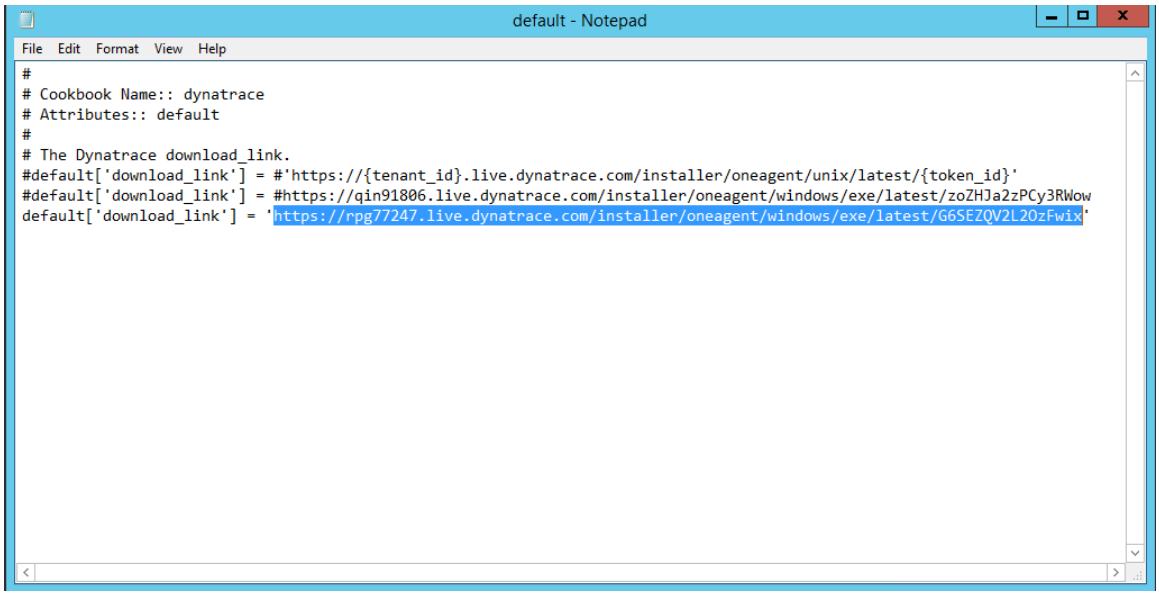


2. After logging in, navigate to **C:\Users\chef-repo\cookbooks\DynatraceOneAgent\attributes** and open the **default.rb** file.

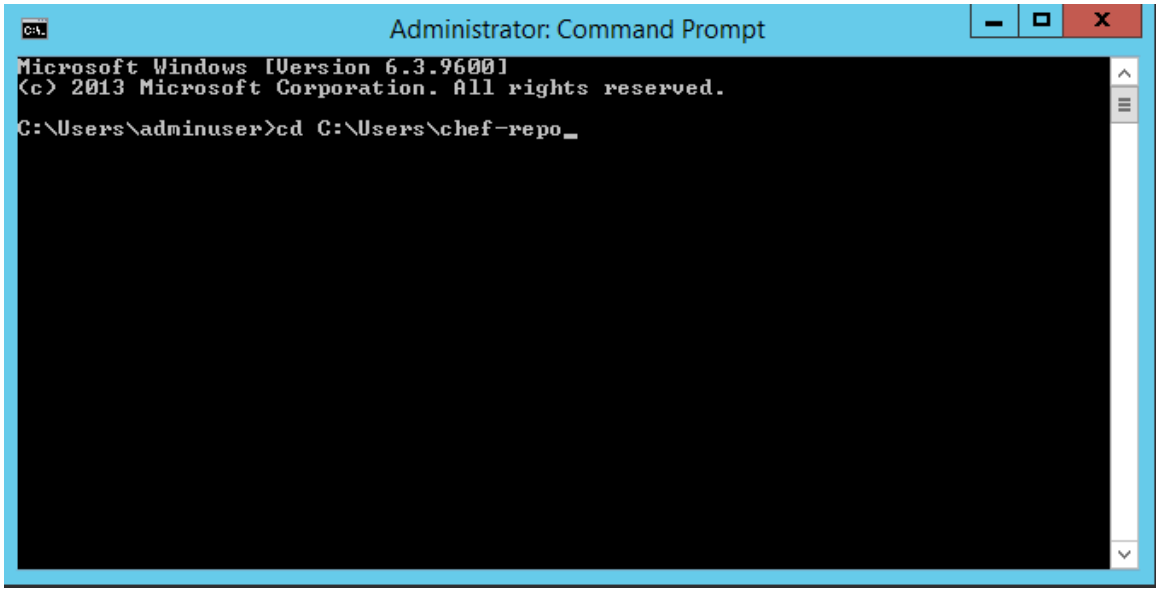


3. Add the new unique url: https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix as the last link and **save** the file.



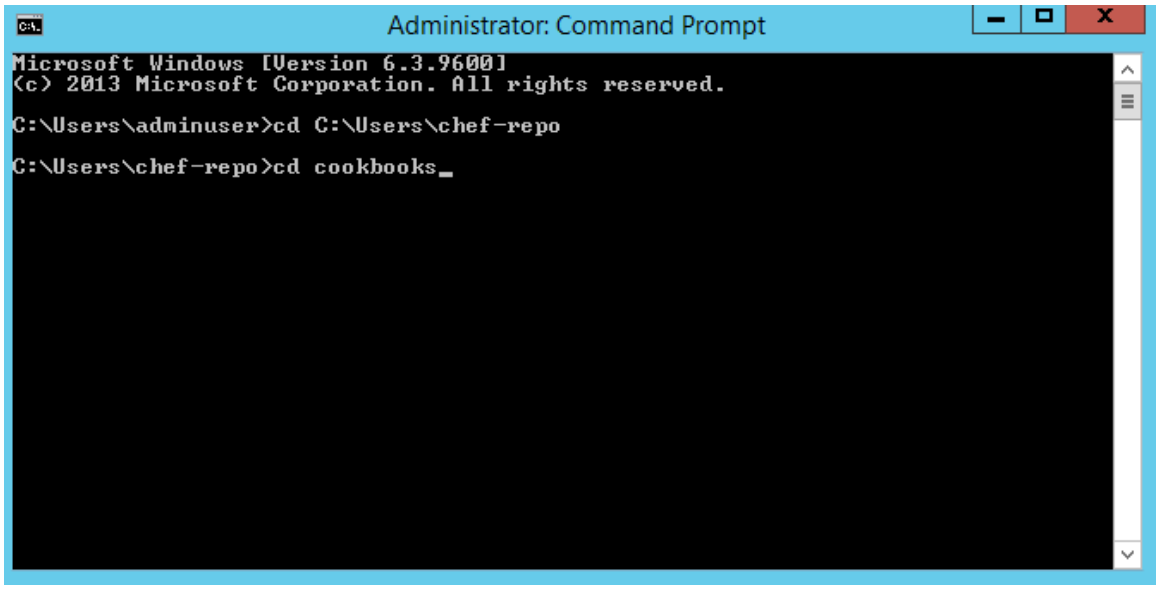


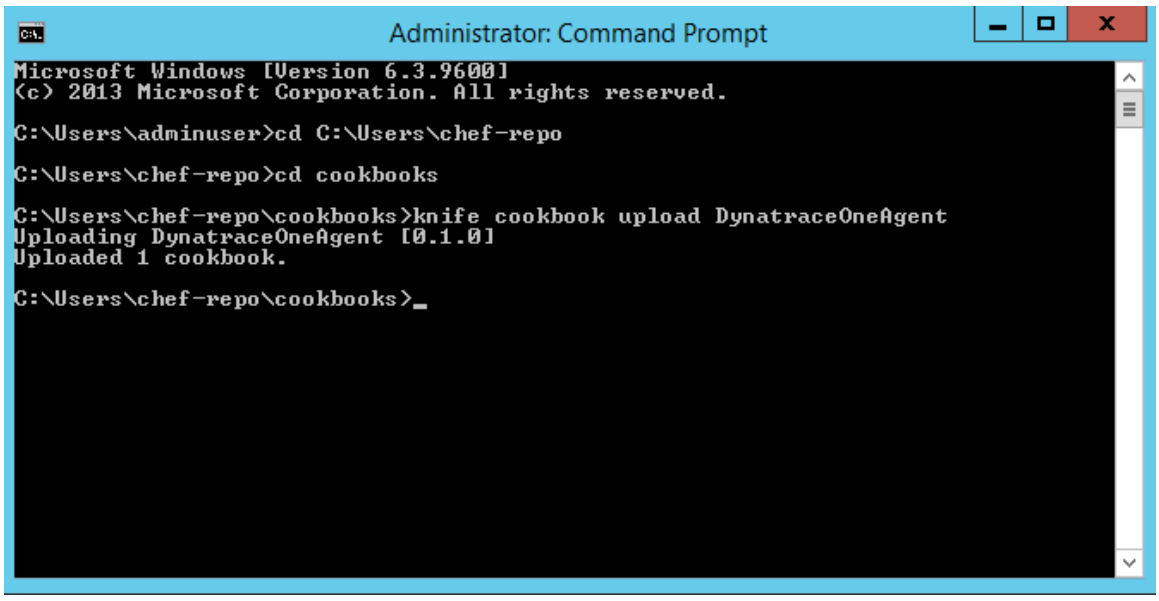
4. Open the command prompt and navigate to **"chef-repo".**



5. Change the directory to **cookbooks** and run the below command to upload the "DynatraceOneAgent":

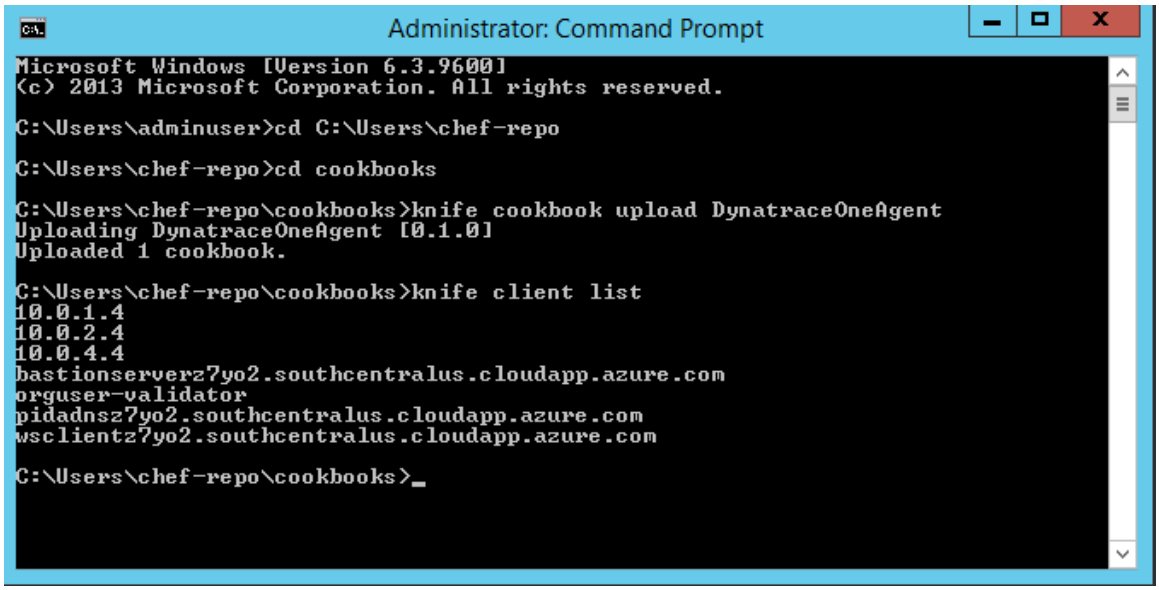
   knife cookbook upload DynatraceOneAgent





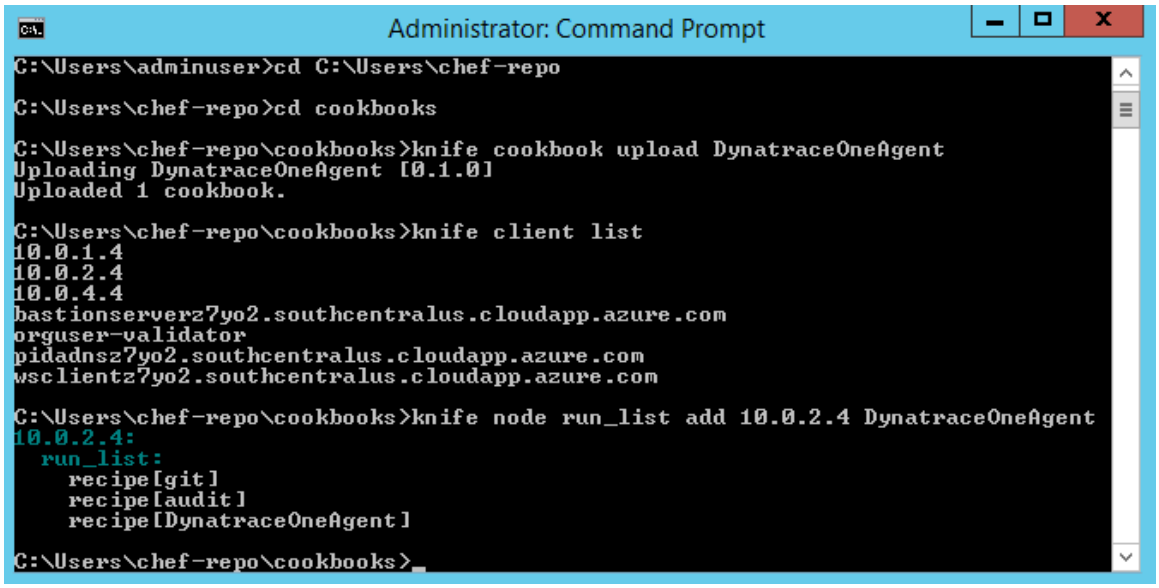
6. Now to check the client on the Chef Workstation, run the below command.

knife client list

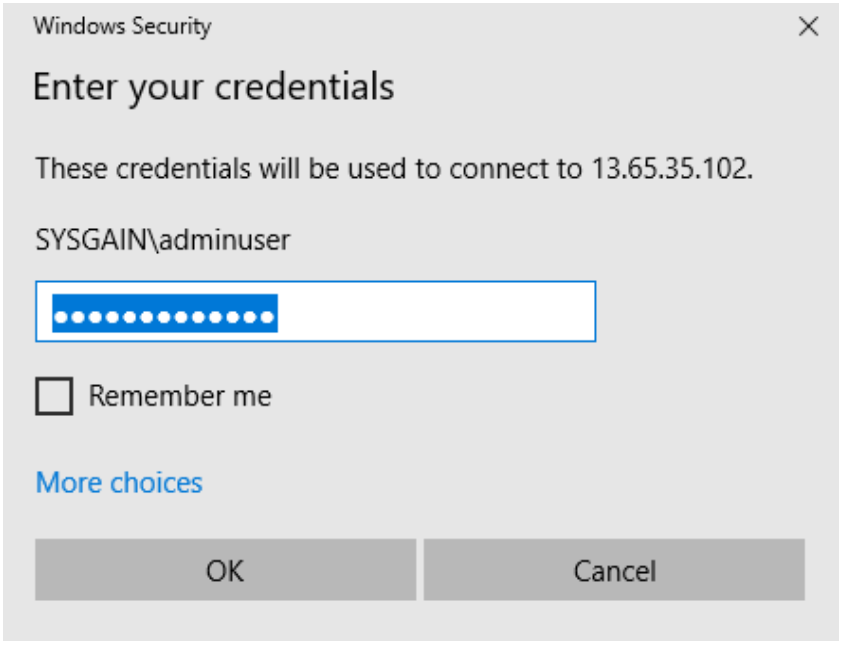


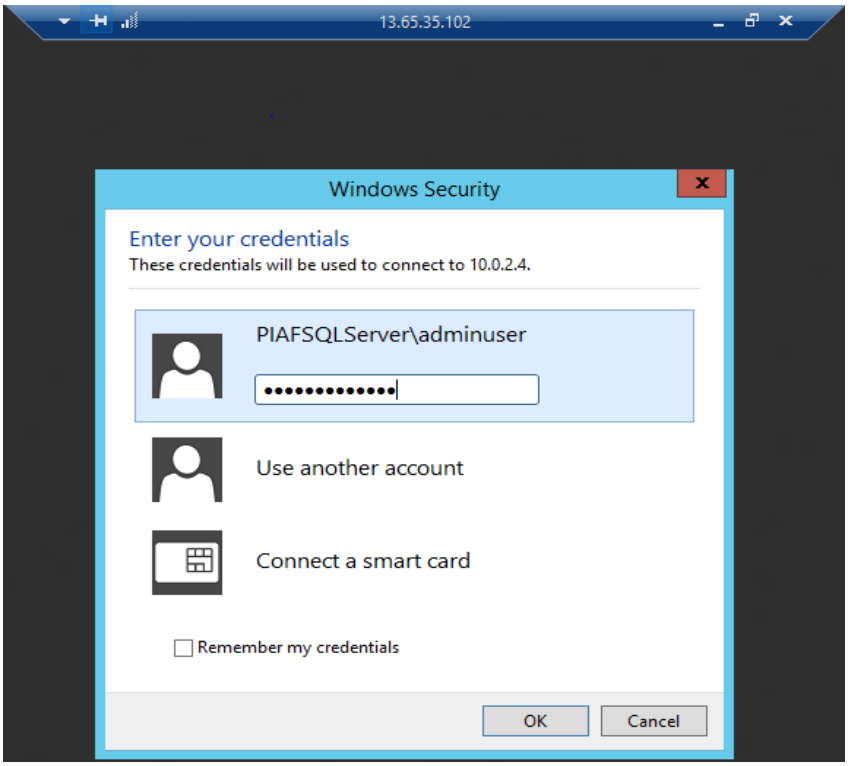
7. Now add the Dynatrace cookbook to the runlist of the targethost (for example, pidadnsw4yjl.westus2.cloudapp.azure.com) using the below command.

knife node run_list add pidadnsw4yjl.westus2.cloudapp.azure.com DynatraceOneAgent

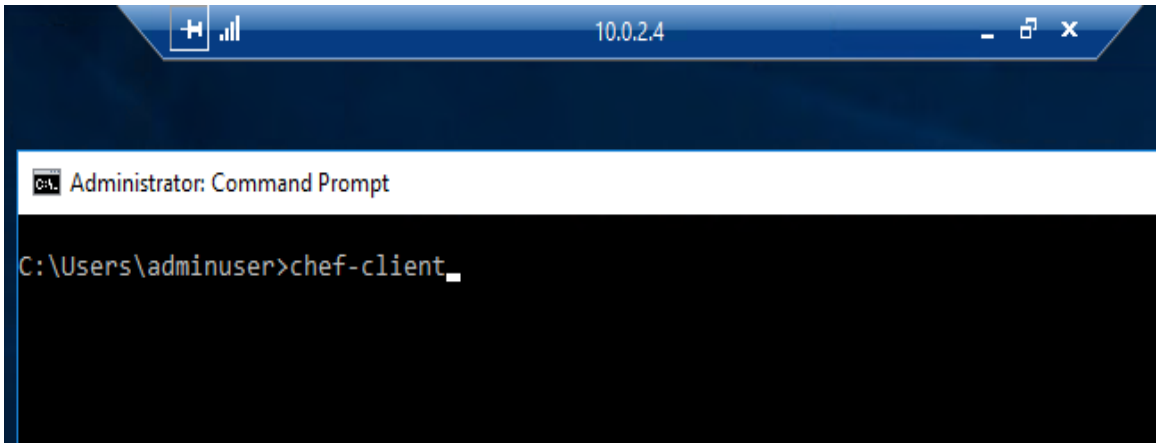


8. Connect to Bastion Server with the user credentials provided in the output section





9. Open the command prompt and run the **"chef-client"** command.

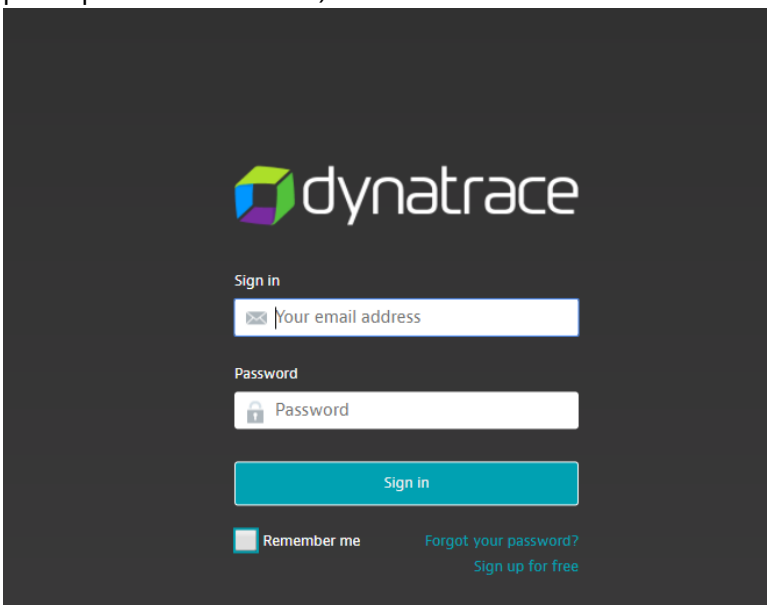

10.0.2.4
Administrator: Command Prompt
C:\Users\adminuser>chef-client

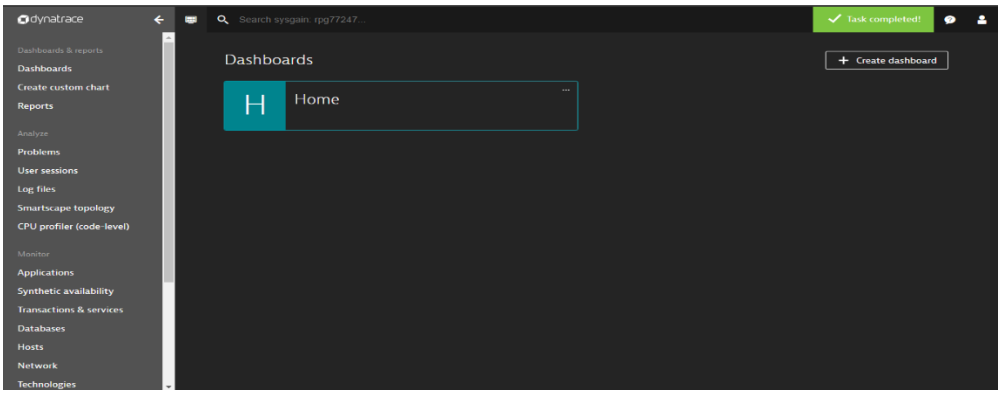
10. After the command is successfully executed, the below output screen will appear.

```
    - install version latest of package DynatraceOneAgent
  * windows_service[Dynatrace OneAgent] action restart[2017-08-16T14:10:56+00:00] INFO: Processing windows_service[Dynat
race OneAgent] action restart (DynatraceOneAgent::oneagent-windows line 28)
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace OneAgent] configured with {:service_name=>"Dynatrace OneAgen
t"}
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace OneAgent] restarted

    - restart service windows_service[Dynatrace OneAgent]
[2017-08-16T14:11:09+00:00] INFO: Chef Run complete in 22.297144 seconds

Running handlers:
[2017-08-16T14:11:09+00:00] INFO: Running report handlers
[2017-08-16T14:11:11+00:00] WARN: Format is json
[2017-08-16T14:11:11+00:00] INFO: Initialize InSpec 1.30.0
[2017-08-16T14:11:12+00:00] INFO: Running tests from: [{:name=>"windows-baseline", :git=>"https://github.com/dev-sec/win
dows-baseline"}]
```

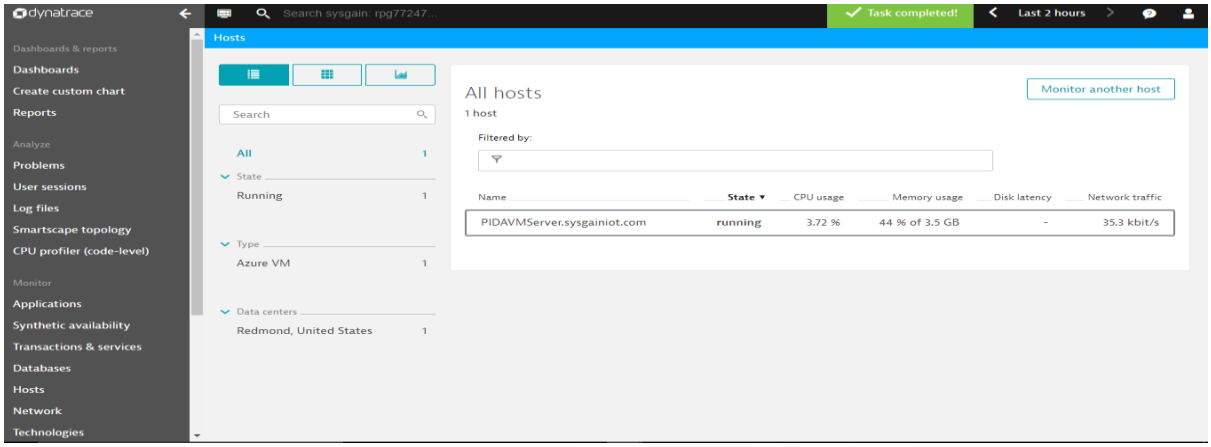
11. Go to the Dynatrace dashboard using the following URL: **https://www.dynatrace.com/**

    Log in to the Dynatrace account using your existing or created account details (which you have created in prerequisites section **4.3**).



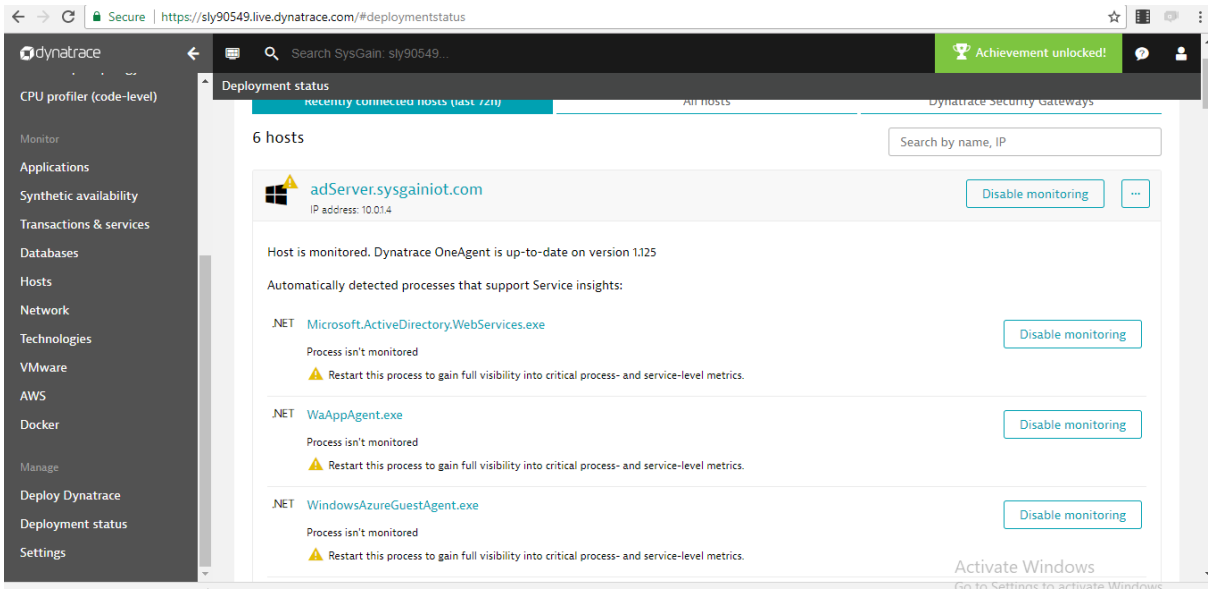


12. From the left side menu select "**Host**". Here you can see the target host added to the Dynatrace Dashboard.

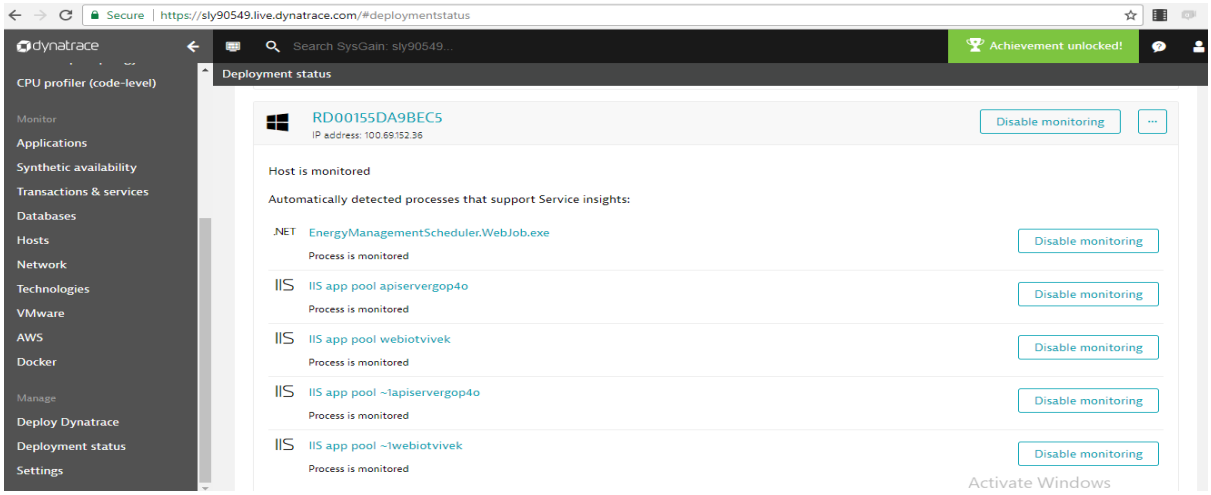


Navigate to **Deployment status** on the left pane of your dashboard page.

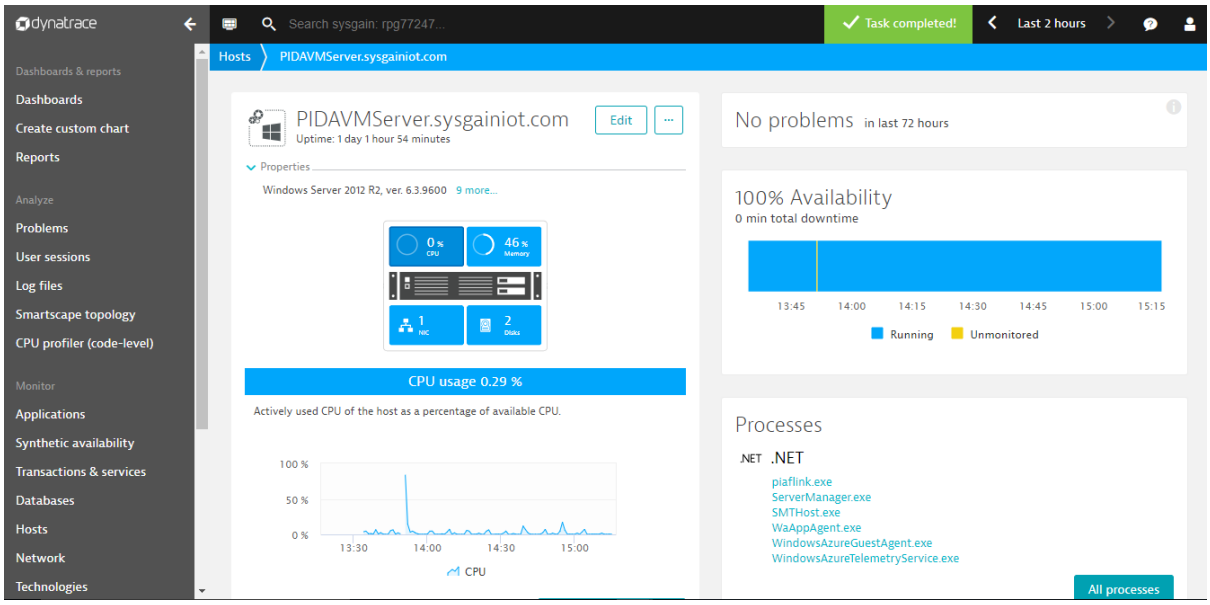
13. Please restart the processors, which need to be monitored.



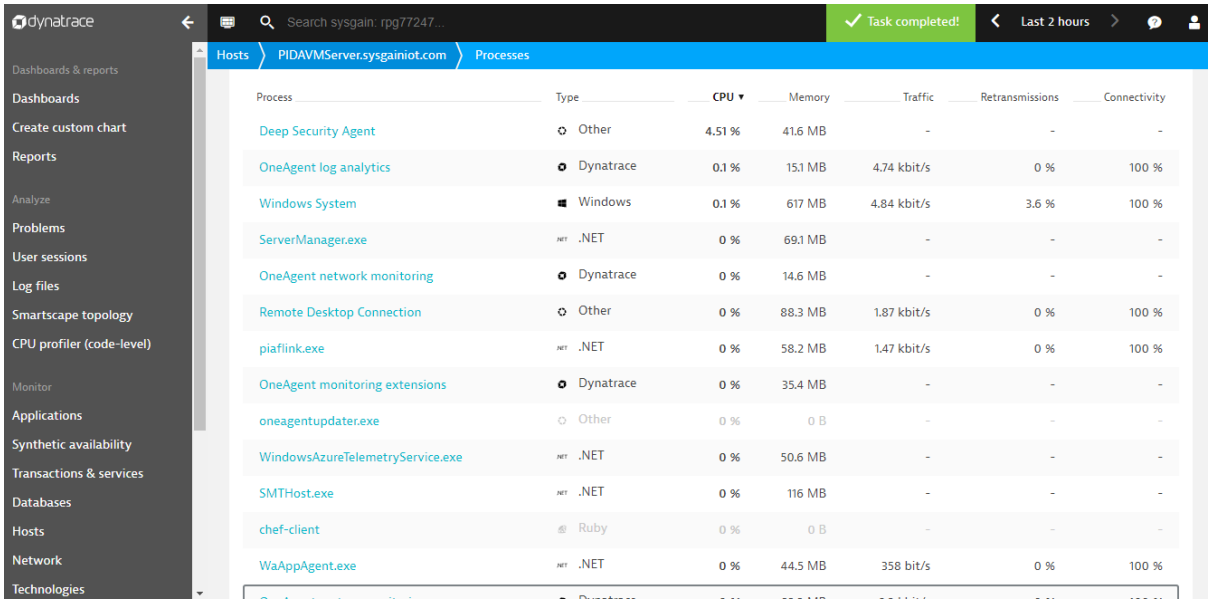
Once restarted, you should be able to see that the processes have started.



14. Each **Host** page details the health of the hardware resources that the selected host relies on. Click one of the four health statistics (**CPU, Memory, Disk,** or **NIC**) to view details of the metrics that contribute to each measurement.

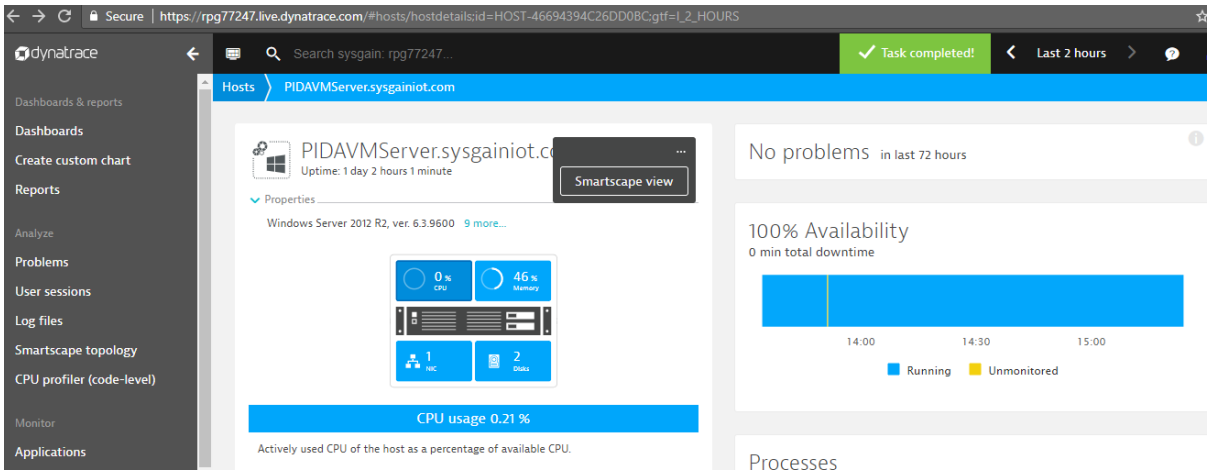


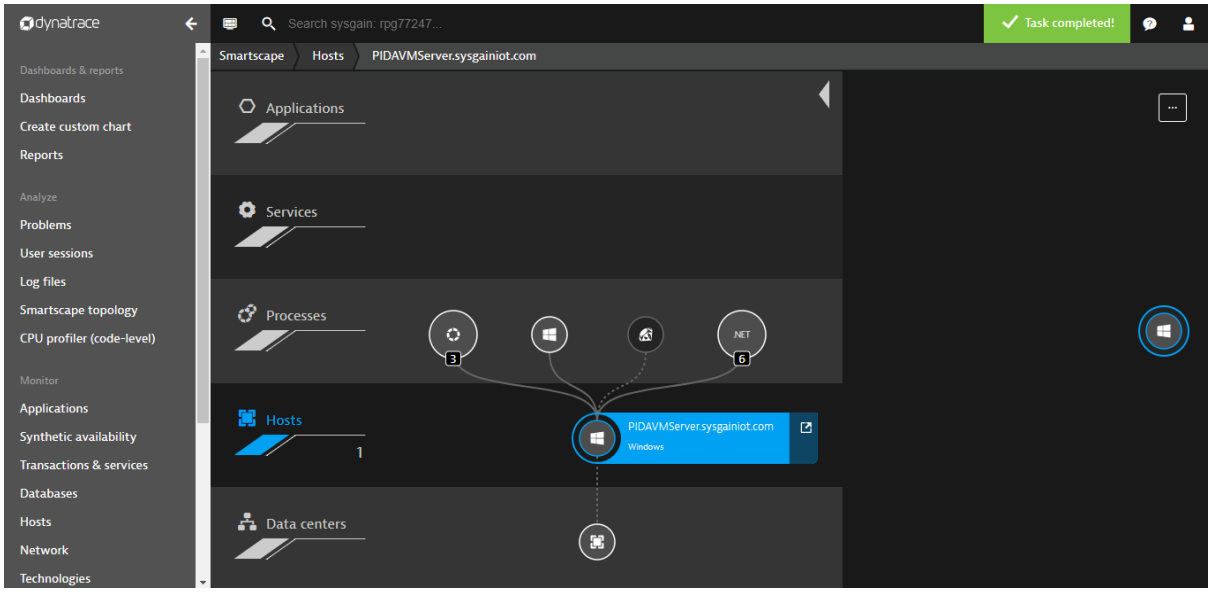
15. Click on "**All processes**", to view the process details running on the host.



16. Dynatrace enables you to visualize the complexities of your application stack and delivery chain with Smartscape technology. In a Smartscape visualization, you can see which individual web page calls which specific web server, the application server that receives the resulting web requests, and where the resulting web request service calls are sent.

17. Select **Smartscape topology** to view various Applications, Services, Processes, Hosts and Data Centers.





7.1.1. Installing Dynatraceoneagent To Web Application (Paas Environment)

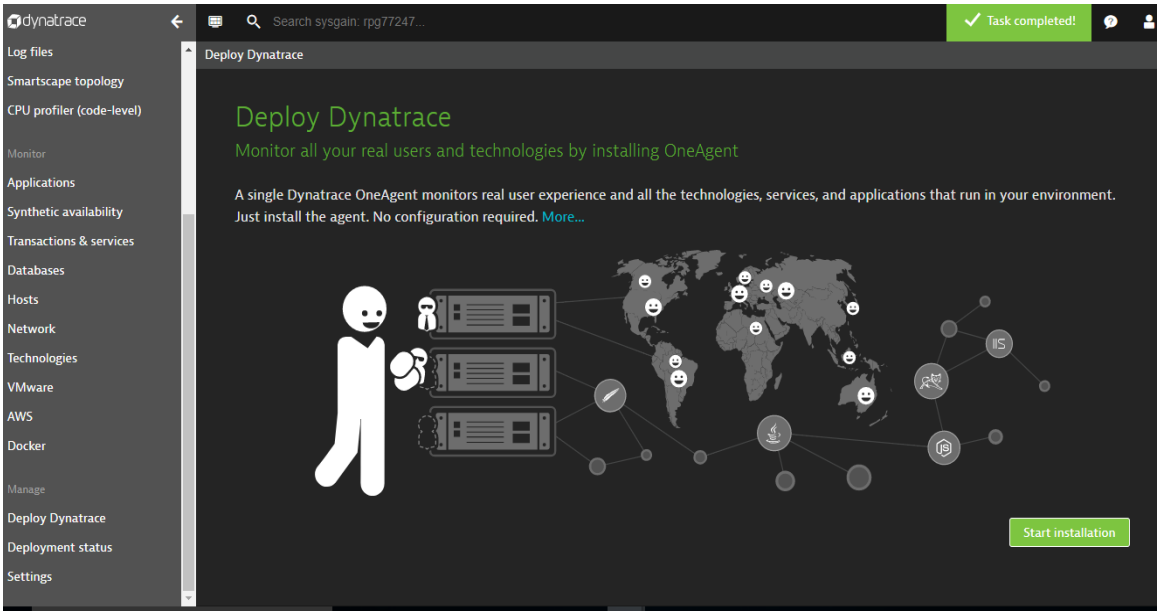
Azure Web Apps is a service provided by Microsoft Azure that gives you the option of deploying and auto-scaling applications and services. Using a predefined Azure site extension, you can modify your deployment by supplying additional resources or packages.

Generate a PaaS token:

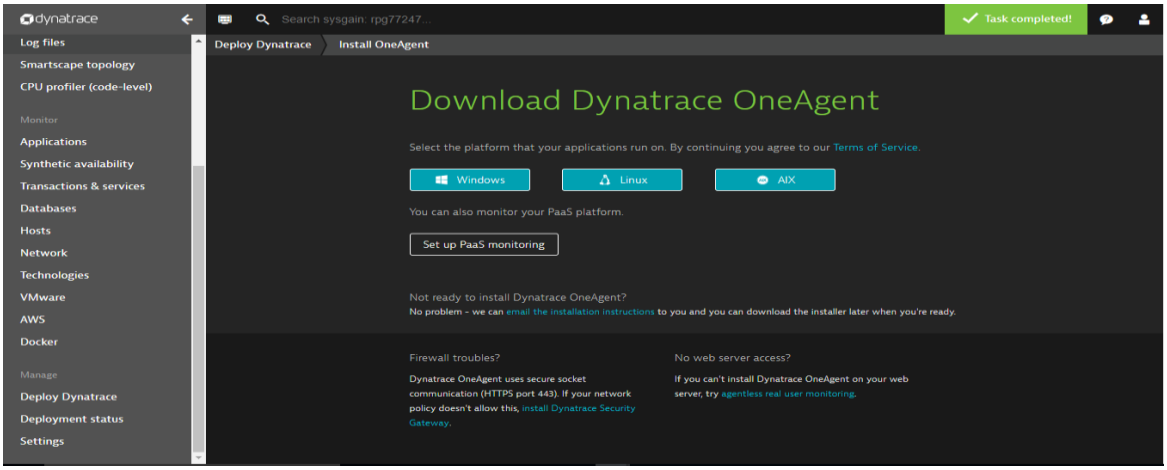
The first step is to get your environment ID and generate a PaaS token for your Dynatrace environment. This information is required so we can map your Azure account to your Dynatrace account.

To get your Dynatrace environment ID and PaaS token:

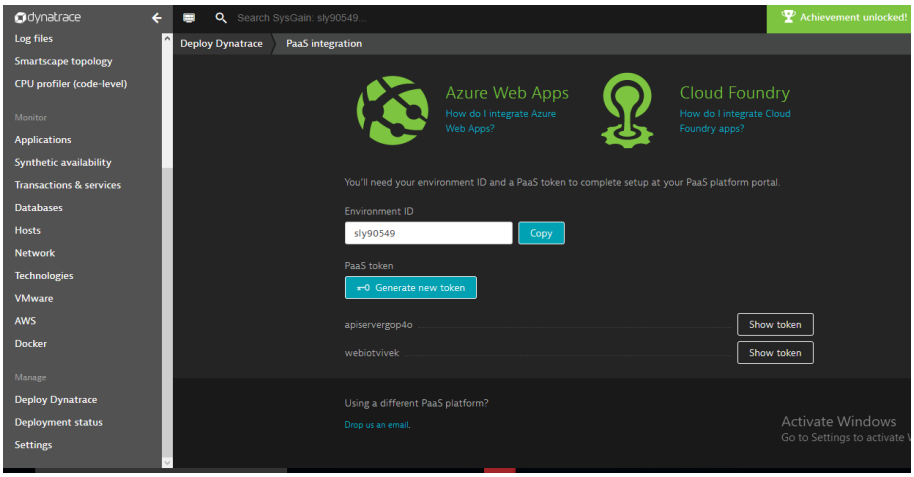
1. Login with your Dynatrace account.
2. Select Deploy Dynatrace from the navigation menu.



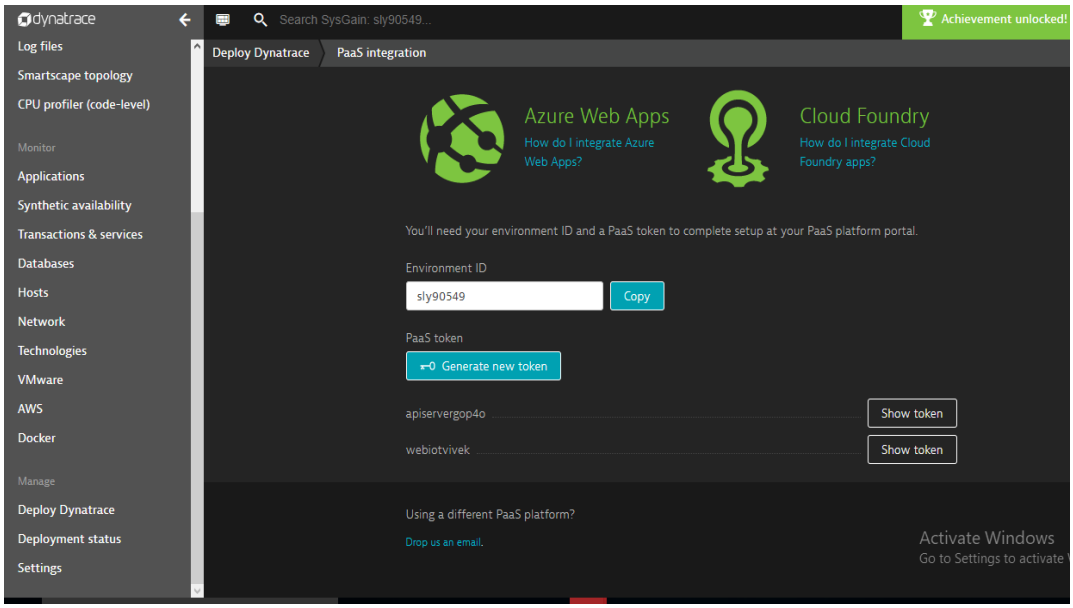
3. Click **Setup PaaS monitoring**.



4. Your environment ID appears in the **Environment ID** text box. You'll need this ID to link your Dynatrace account with your PaaS environment. Click **Copy** to copy the ID to the clipboard. You can do this at any time by revisiting this page.



5. To generate a PaaS token, click the **Generate new token** button. The PaaS token is essentially an API token that's used in combination with your environment ID to download Dynatrace OneAgent.



6. Type in a meaningful name for your PaaS token. A meaningful token name might be the name of the PaaS platform you want to monitor (for example: azure, cloud-foundry, or openshift). To view and manage your existing PaaS tokens, go to **Settings > Integration > Platform as a Service**.

- In the screenshots, we have now generated a PasS token for token name "webiovivek".

7. Click **Generate** to create the PaaS token. The newly created PaaS token will appear in the list below. Click **Copy** to copy the generated token to the clipboard. You can do this at any time by revisiting this page and clicking **Show token** next to the relevant PaaS token.
   - The sample token generated: **3o2WgxoYSH6-9y5NX2GS-**

Configure the Dynatrace Site Extension via the Azure portal

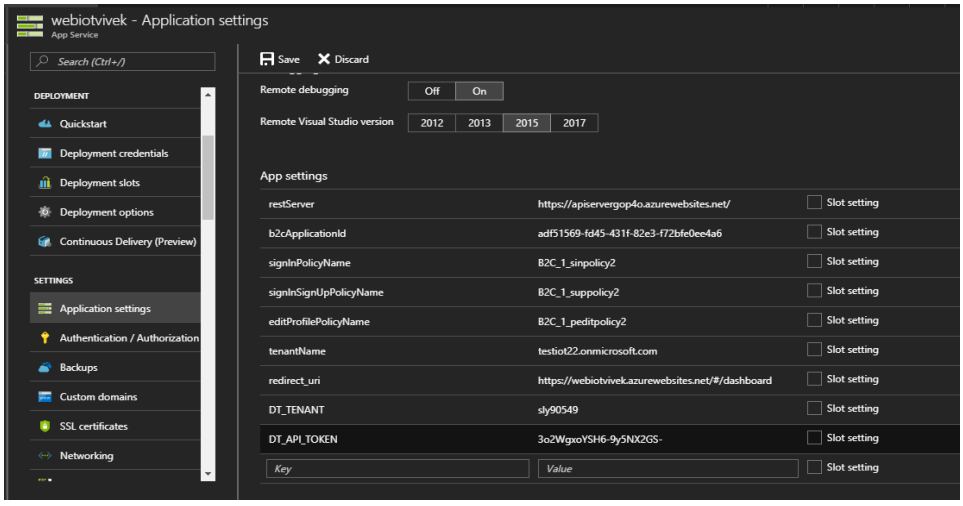
1. Now, open **portal.azure.com** in a new browser window.

2. Navigate to the web app in the resource group you want to monitor.

3. From **Settings**, select **Application Settings**. Then, scroll down to the App Settings area and add two new **Key/Value** pairs:

4. **DT_TENANT**: Your environment ID, as shown above.

5. **DT_API_TOKEN**: Copy and paste the PaaS token from the Download Dynatrace page shown above. https://help.dynatrace.com/images/content/infrastructure-monitoring/paas/portal.png.



Install the Dynatrace Azure site extension

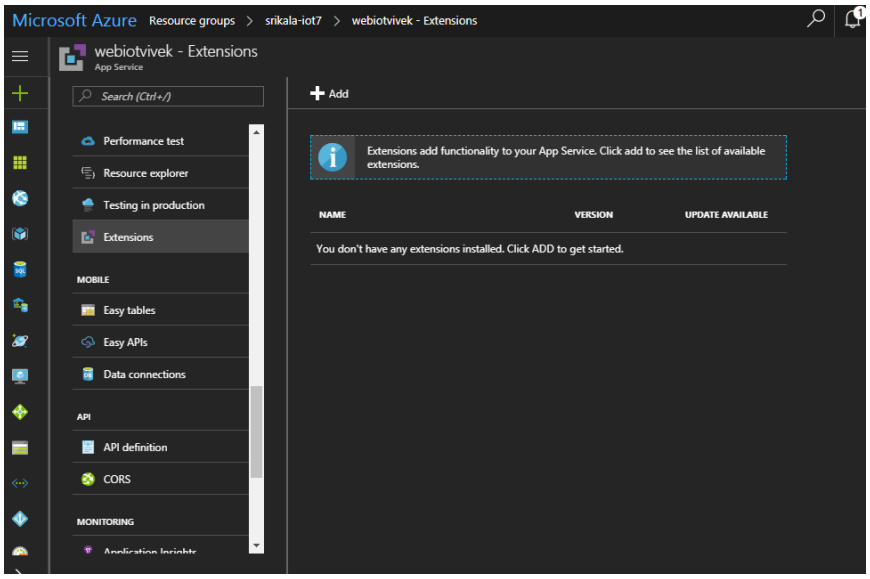
To do this via the Azure Portal, follow the below steps:

1. Open **portal.azure.com** in a new browser window.

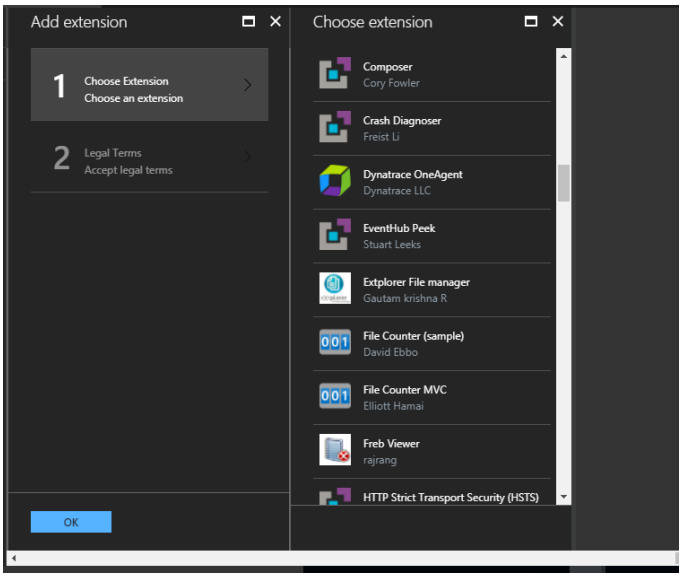
2. Navigate to the web app you want to monitor.

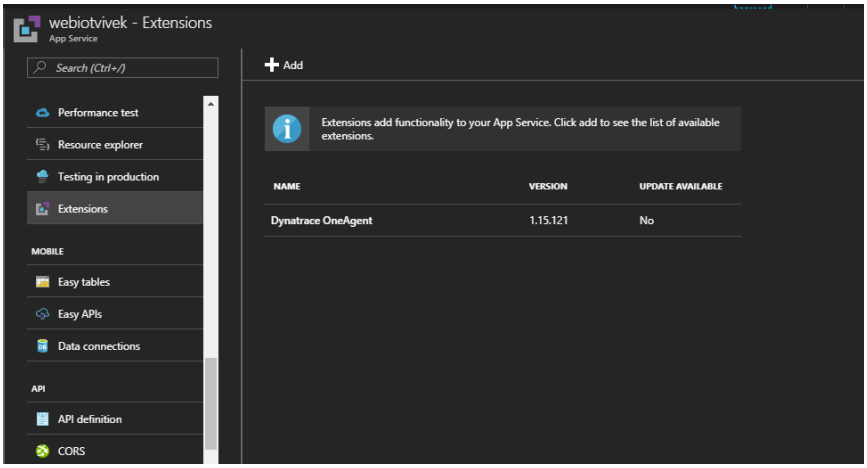
3. Select **Extensions** from the list of options. You'll find this in the **Development tools** subsection (note the **Search** field at the top of the page in case you have trouble finding this option).

4. Within the new pane (i.e., "blade" in Azure terminology) that appears on the right-hand side, click **Add**.

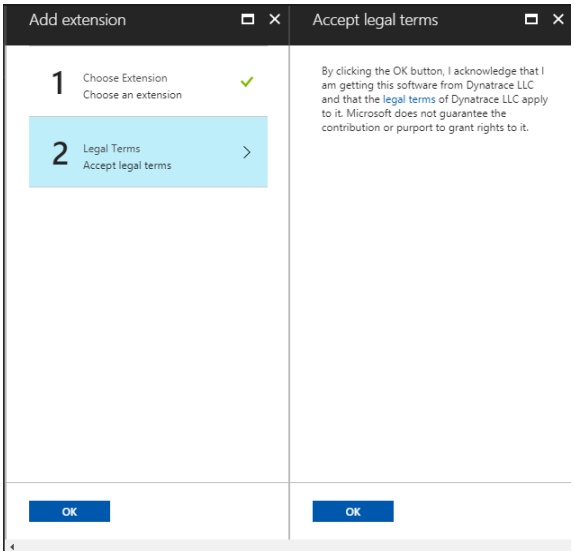


5. Scroll through the list until you find **Dynatrace OneAgent**. Note that entries are not ordered alphabetically. https://help.dynatrace.com/images/content/infrastructure-monitoring/paas/extension.png

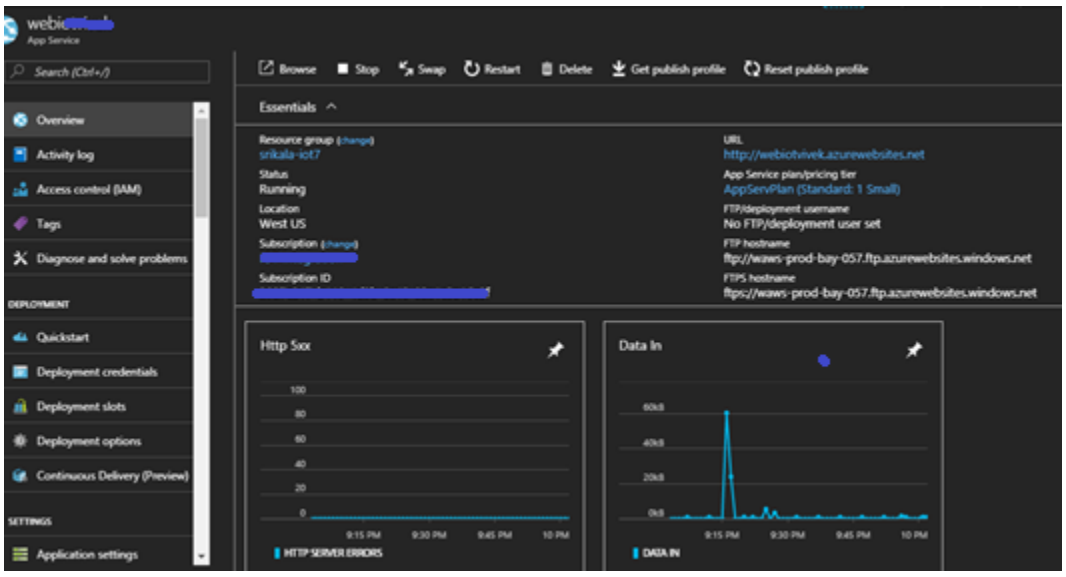

Add extension
1
Choose Extension
Choose an extension
2
Legal Terms
Accept legal terms
OK
Choose extension
Composer
Cory Fowler
Crash Diagnoser
Freist Li
Dynatrace OneAgent
Dynatrace LLC
EventHub Peek
Stuart Leeks
Extplorer File manager
Gautam krishna R
File Counter (sample)
David Ebbo
File Counter MVC
Elliott Hamai
Freb Viewer
rajrang
HTTP Strict Transport Security (HSTS)


webiotvivek - Extensions
App Service
Search (Ctrl+/)
Performance test
Resource explorer
Testing in production
Extensions
MOBILE
Easy tables
Easy APIs
Data connections
API
API definition
CORS
Add
Extensions add functionality to your App Service. Click add to see the list of available extensions.
NAME
VERSION
UPDATE AVAILABLE
Dynatrace OneAgent
1.15.121
No

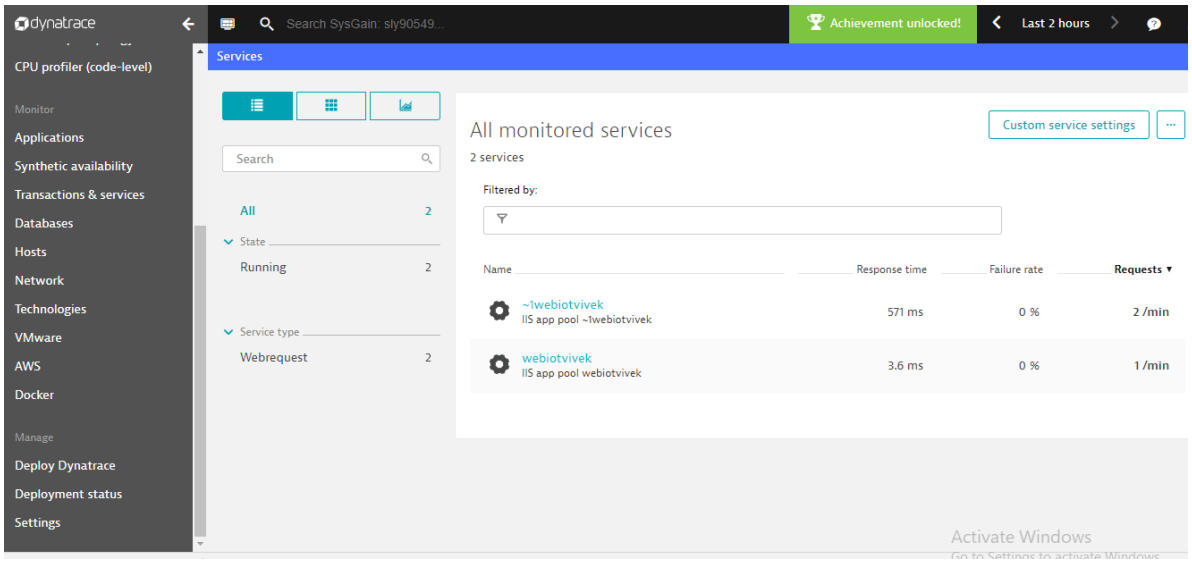
6. Click **OK** to apply Dynatrace monitoring to your Azure website.



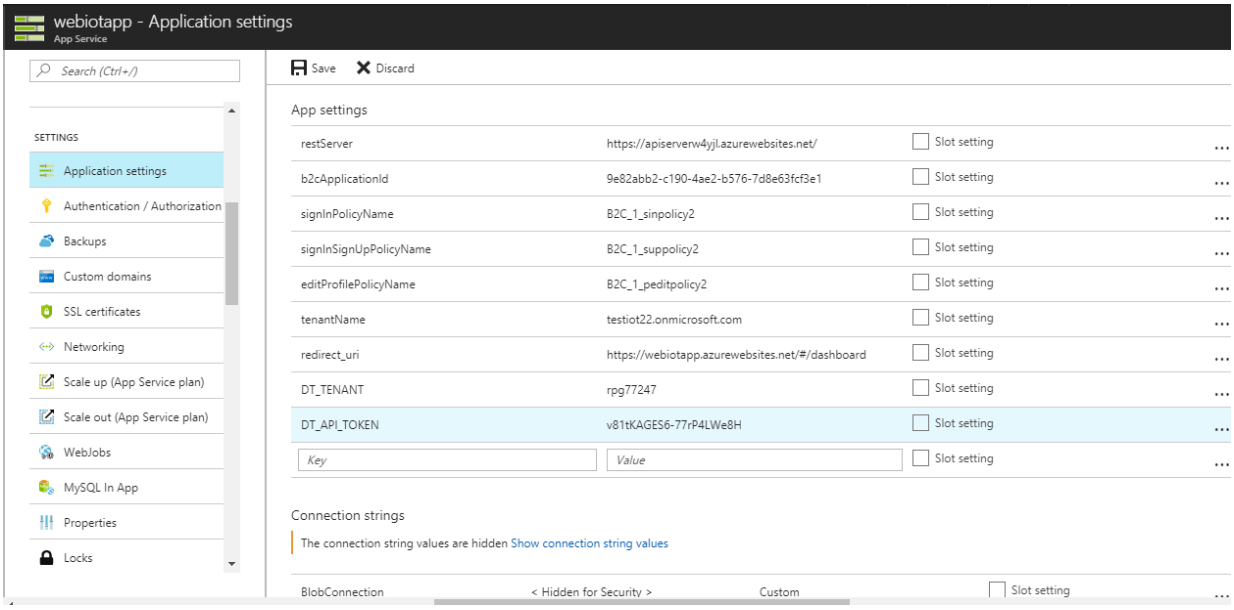
7. Restart your website so that Dynatrace begins to receive monitoring data. Following a restart, you should see the hosts and services that you've set up via your Azure service plan (see example below). Note that the **PaaS type** setting is set to Azure.



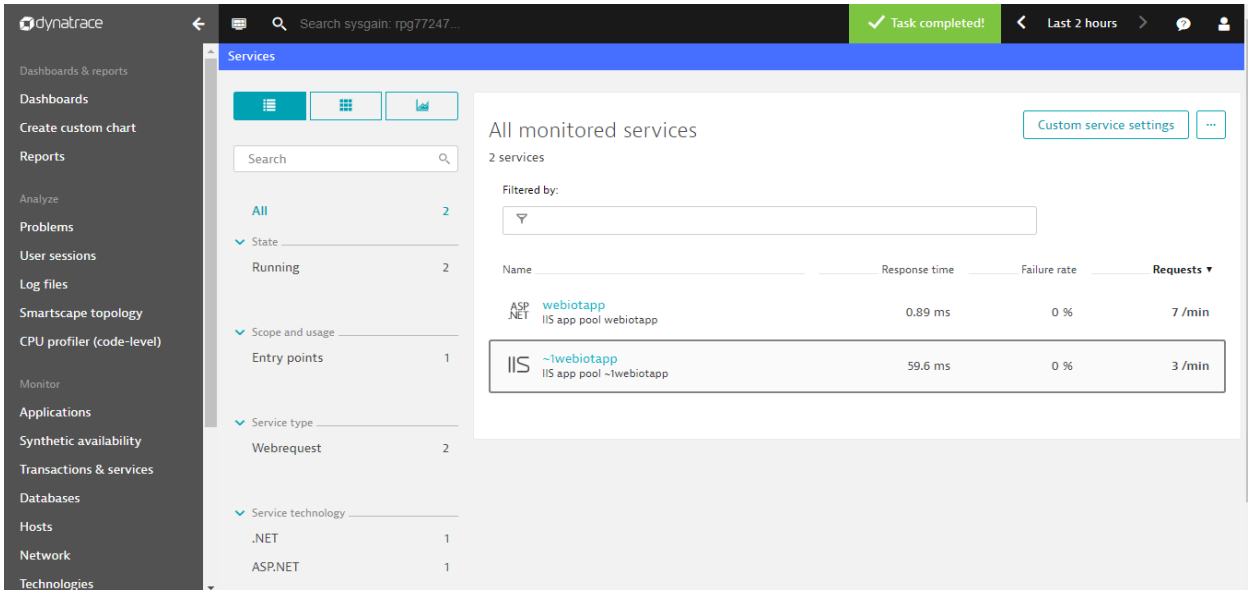
8. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added



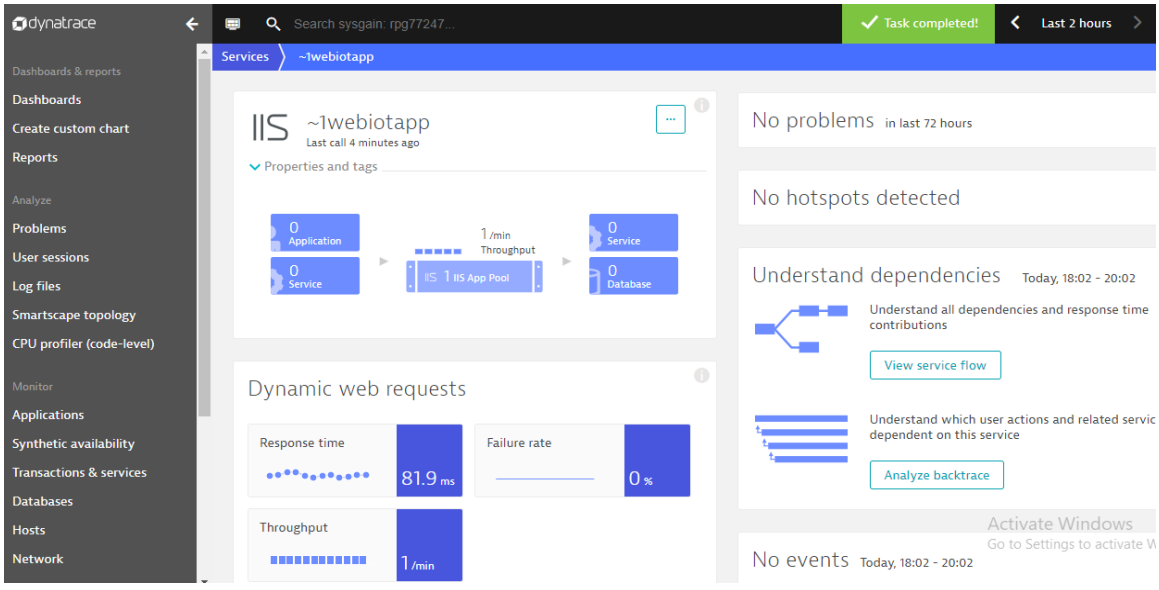
9. Click on the application to get Metrics for the application.

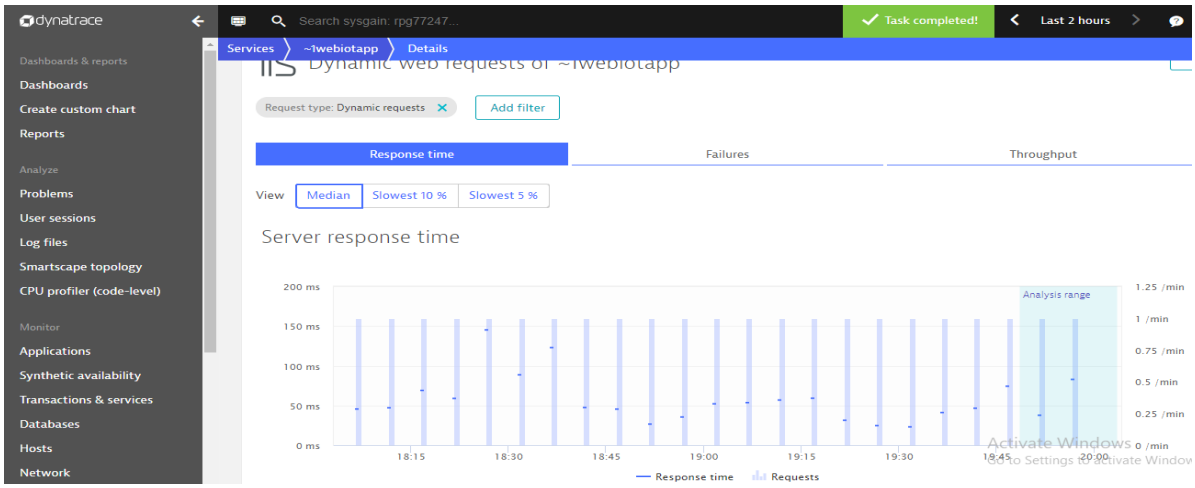


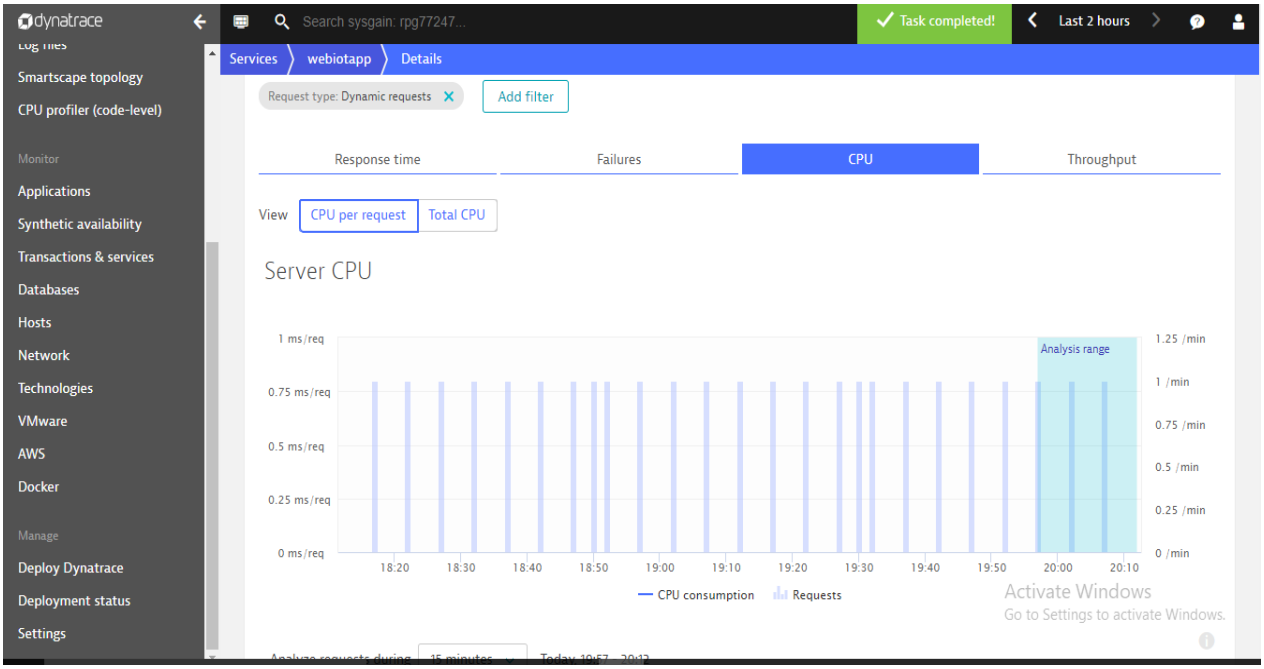
10. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added.



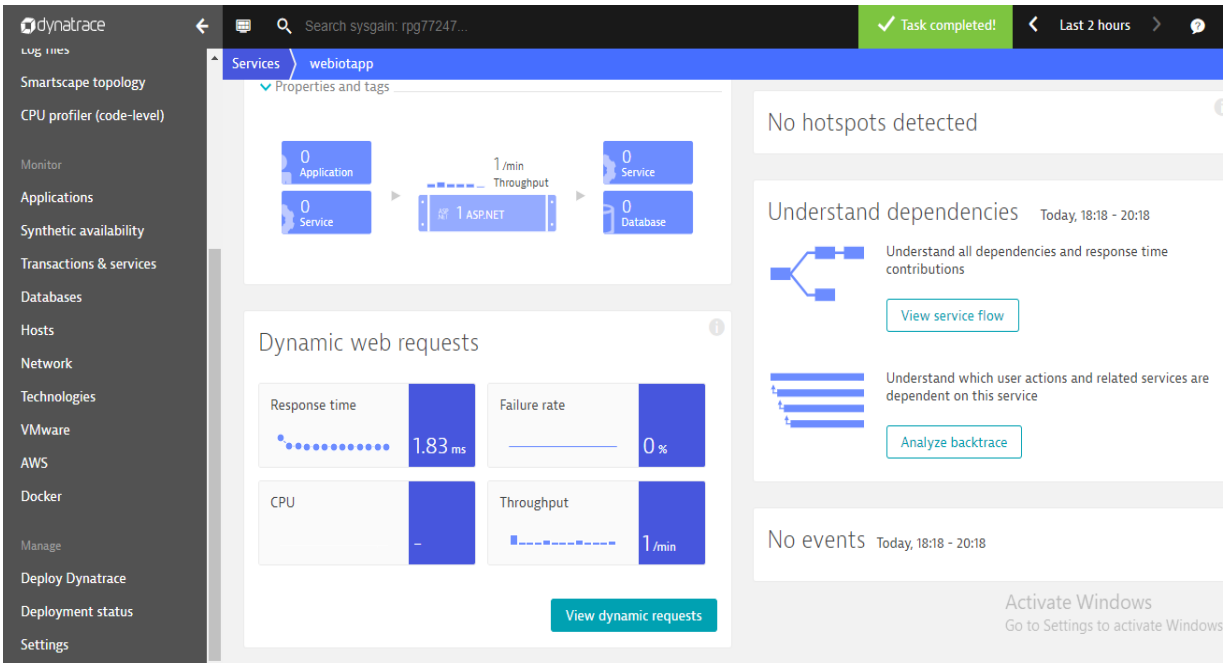
11. Click on the "Response time", "Failure rate", "Throughput", "CPU" to get more detailed metrics.

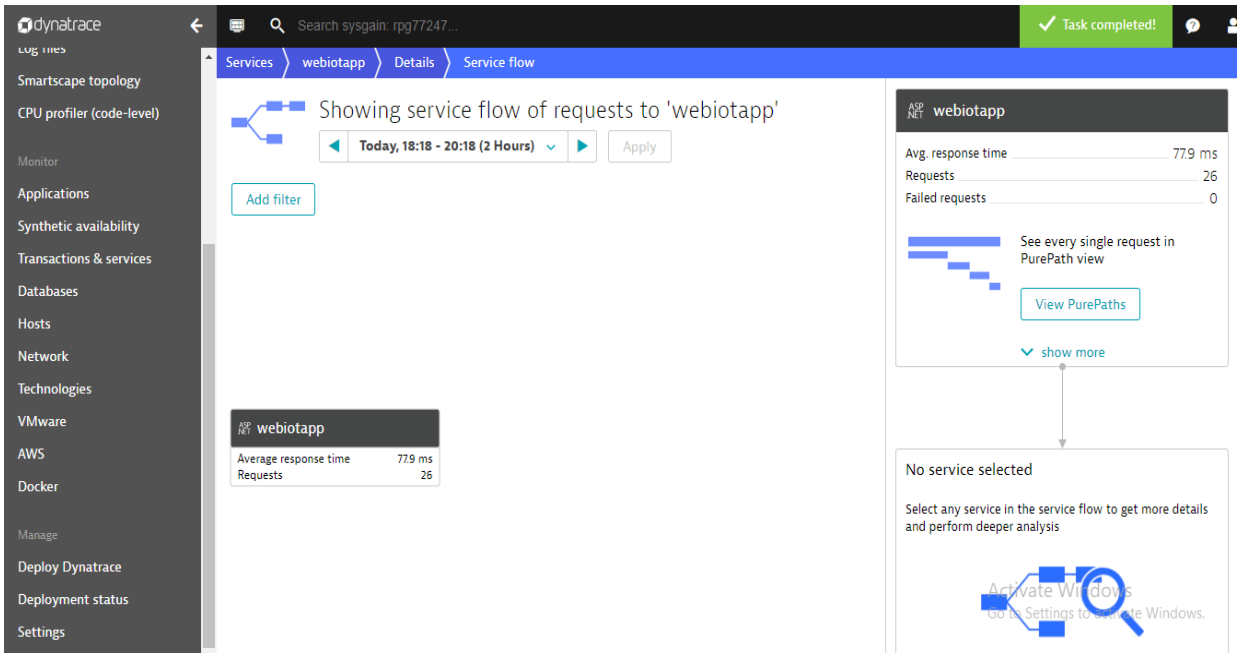




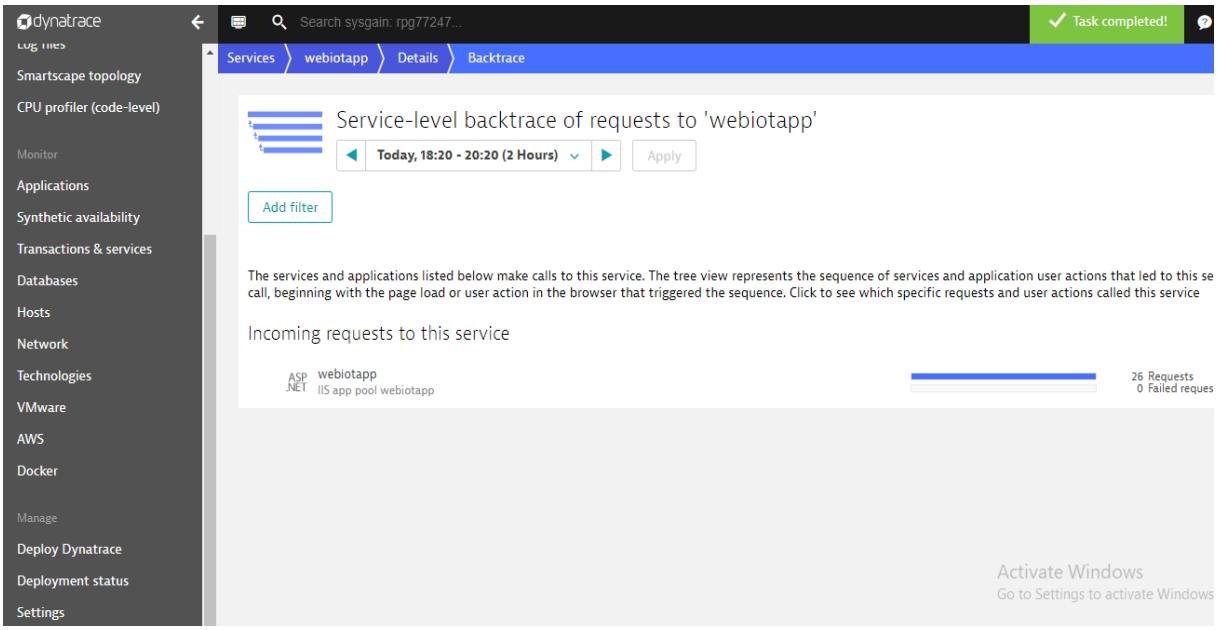


12. To understand all dependencies and response time contributions, Click **View service flow** from the application page





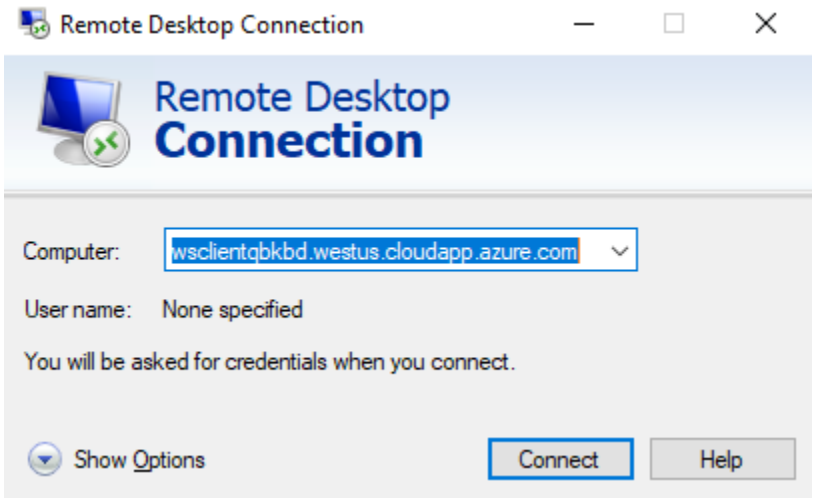
13. To understand which user actions and related services are dependent on this service, Click **Analyze backtrace**.



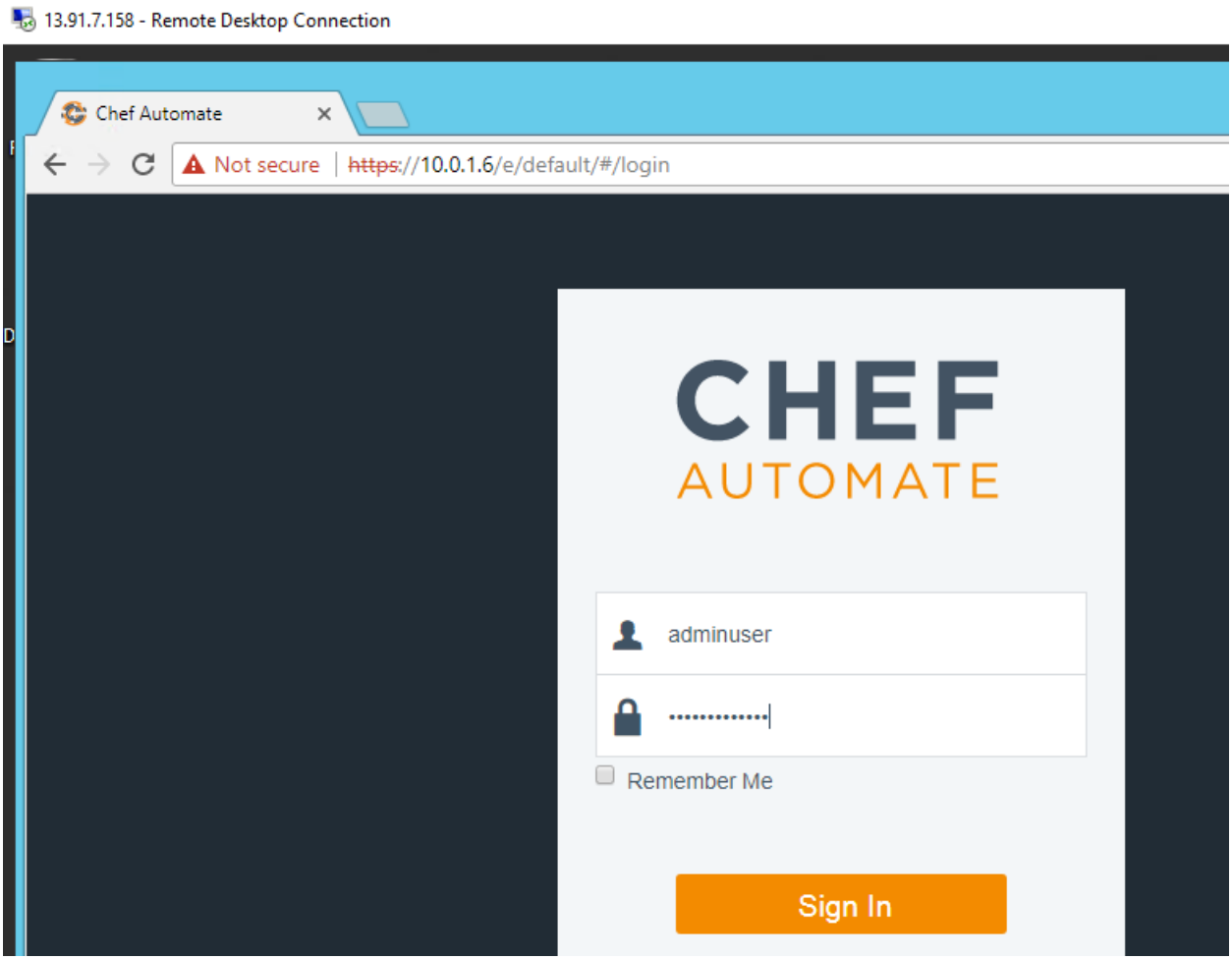
7.2. Chef Automate

To check the installed nodes status.

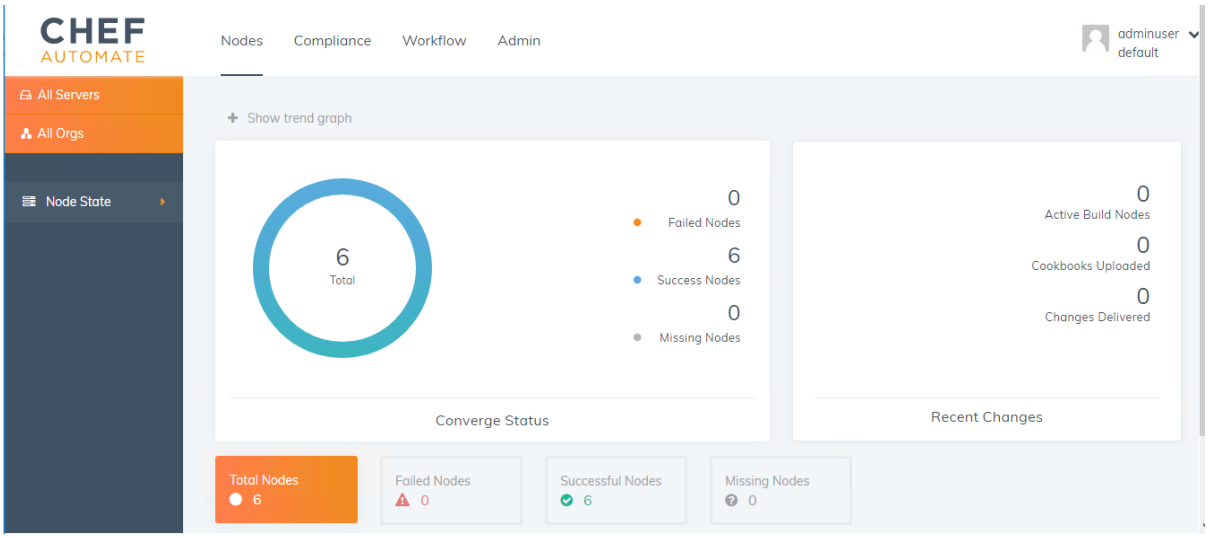
1. Using **workstationFQDN,** Login to the ChefWorkStation with **adminUsername** provided in the outputs section and password as **adminPassword** used during template deployment.

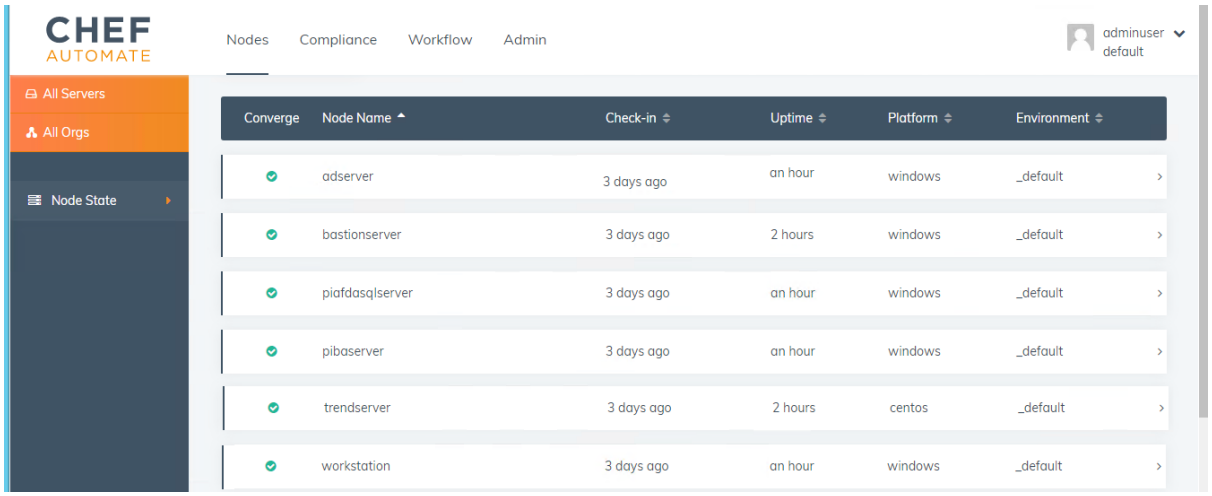


2. Copy and paste the **chefAutomateIPAddress** in a browser which is provided in the outputs section.Login with the **chefAutomateLoginUsername** and **adminPassword** used during template deployment.



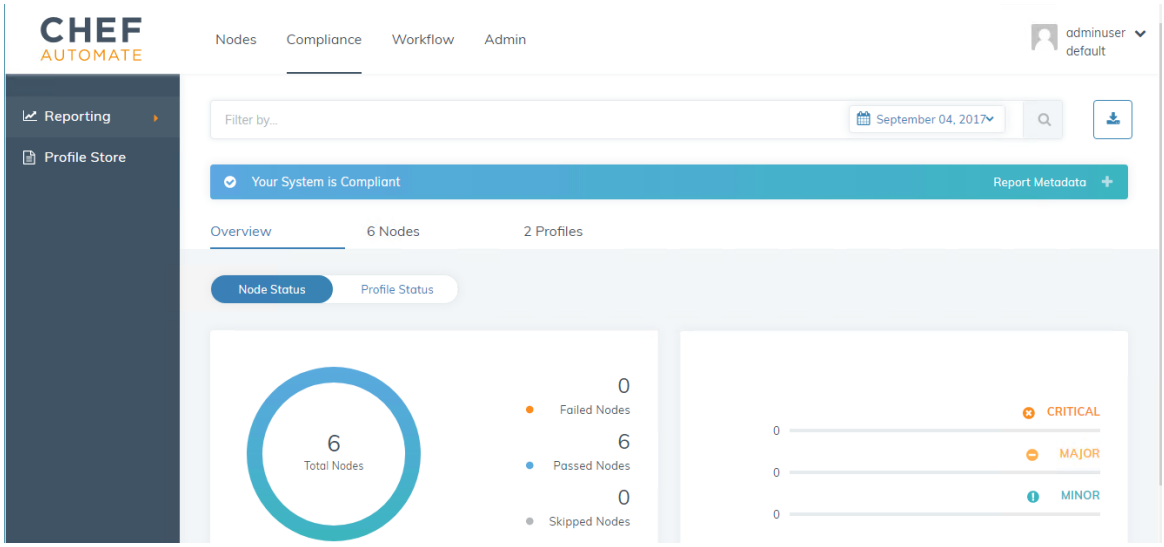
3. All the nodes which are added to Chef are listed under Nodes section.



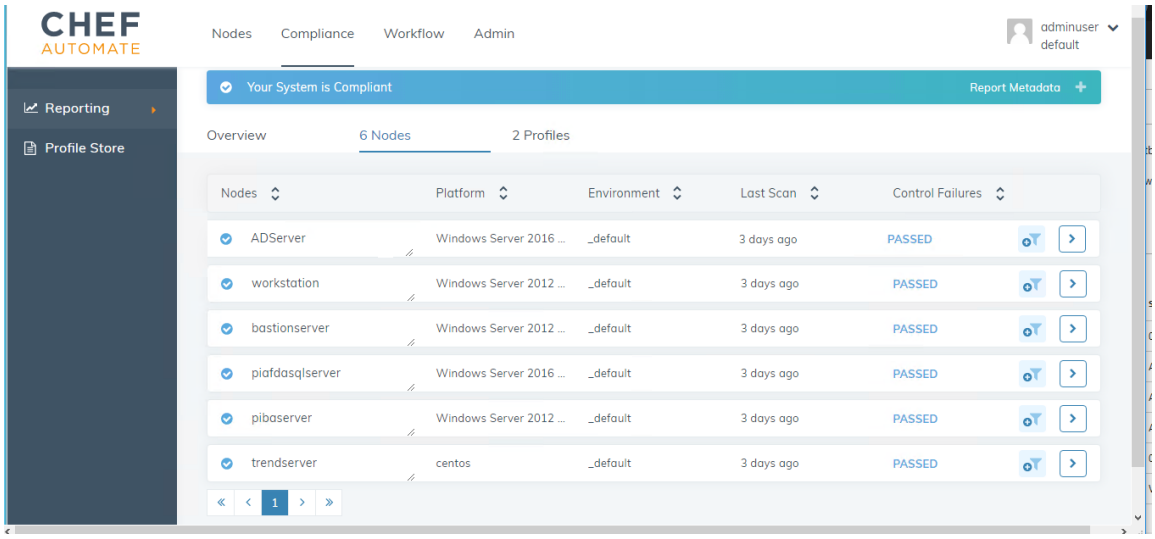


4. Click on **Compliance** blade to view the Control Failures of each node.

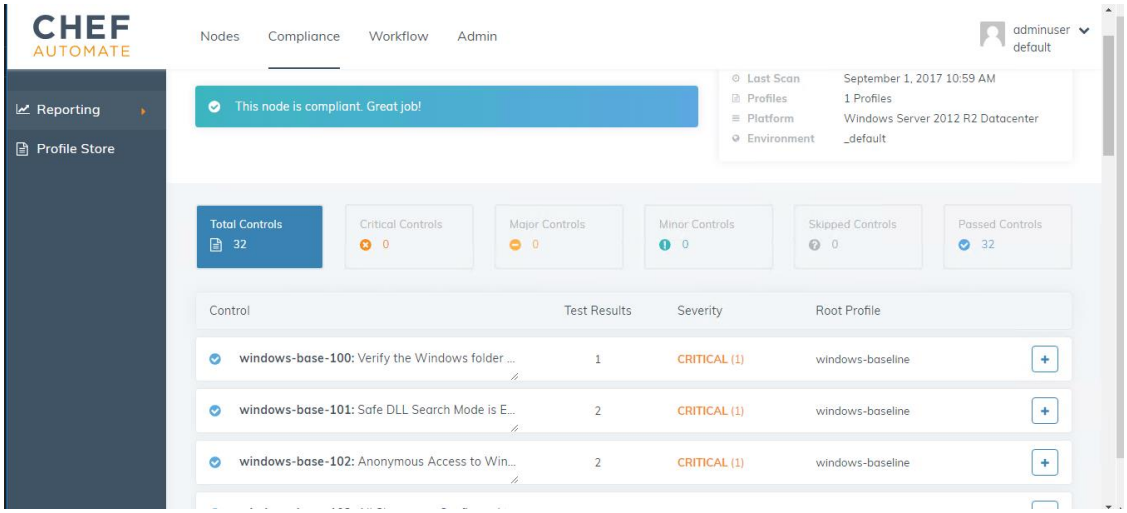
You can see the all nodes are passed and there are no failures are present. In chef Automate for compliance failures Nodes are scanned by audit(windows) and audit-linux(Linux nodes) cookbooks and the failures will fixed by applying windows-hardening and os-hardening (Linux) cookbooks. This process is automated in our system, so that you can see all nodes are non-compliance.



5. Click on nodes tab in compliance page to view list of nodes and status of nodes



6. Select any one node to view the failed or passed controls of nodes individually

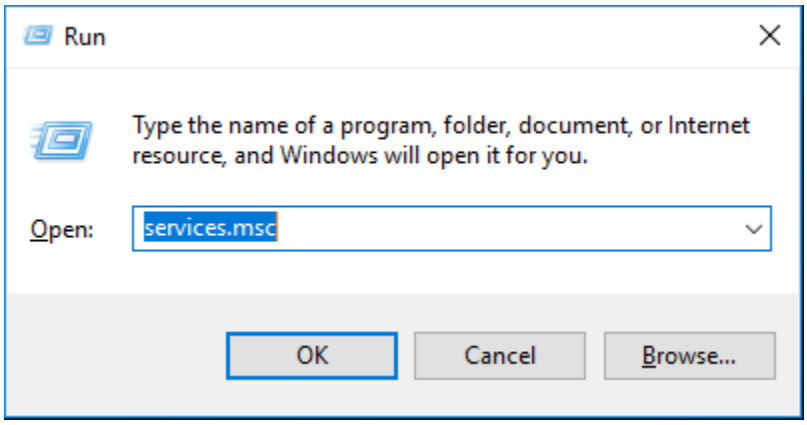


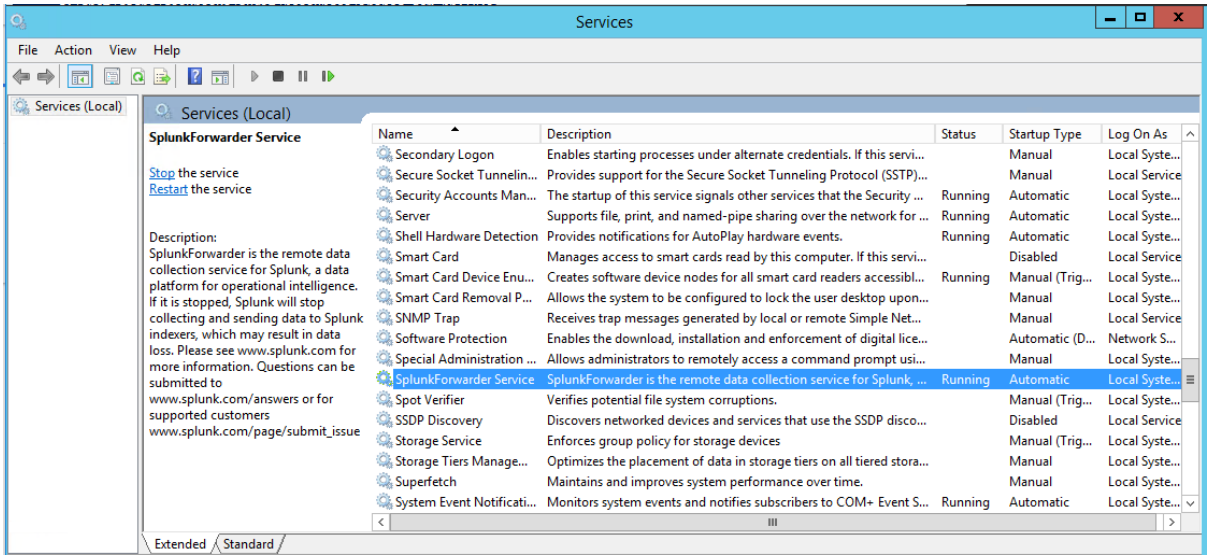
Splunk Universal Forwarder Installation Using Chef Automate:

Spunk universal Forwarder software is used to forward the widows event logs to the splunk server. Splunk forwarder installation and configuration in all windows servers are automated by chef automate, for this we have Splunk-uf-install cookbook it will installs the splunk forwarder and also forwards the windows evet logs to the spunk server.

Checking the Splunk forwarder installation status in client server:

Login to client machine and Run services.msc and check the splunk forwarder service status in services window





You can see splunk forwarder service is running successfully, after applying the splunk-uf-install cookbook on windows server it will forwards all existing logs to the splunk server and whenever new event occurred in server it will automatically forwards the new log to the splunk server

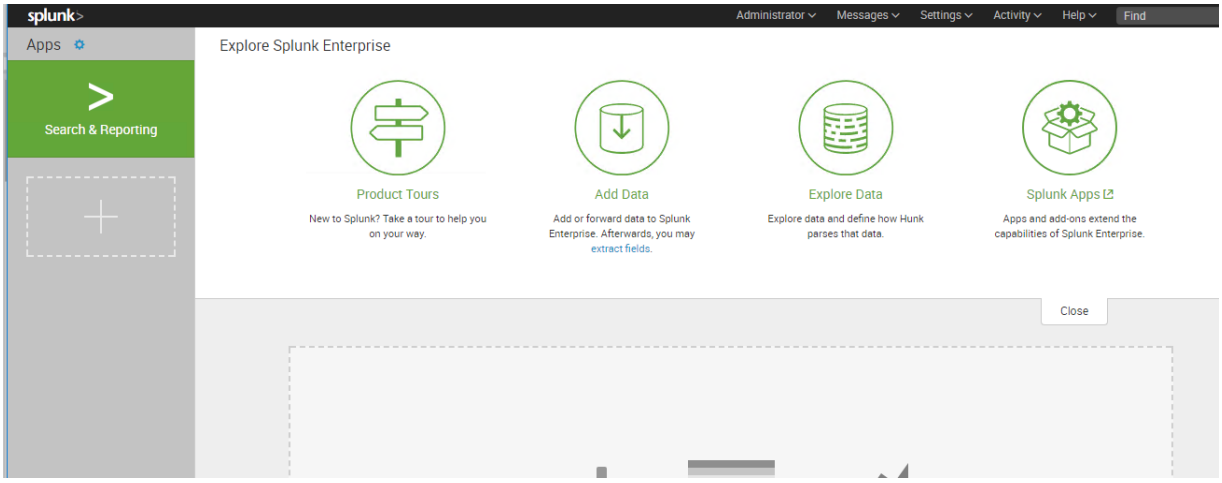
7.3. Splunk

Splunk offers the best platform for log analytics. Splunk produces software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface. It is exceptionally strong in dealing with today's large volumes of data, Splunk provides acute efficiency to search, analyze, store and process data.

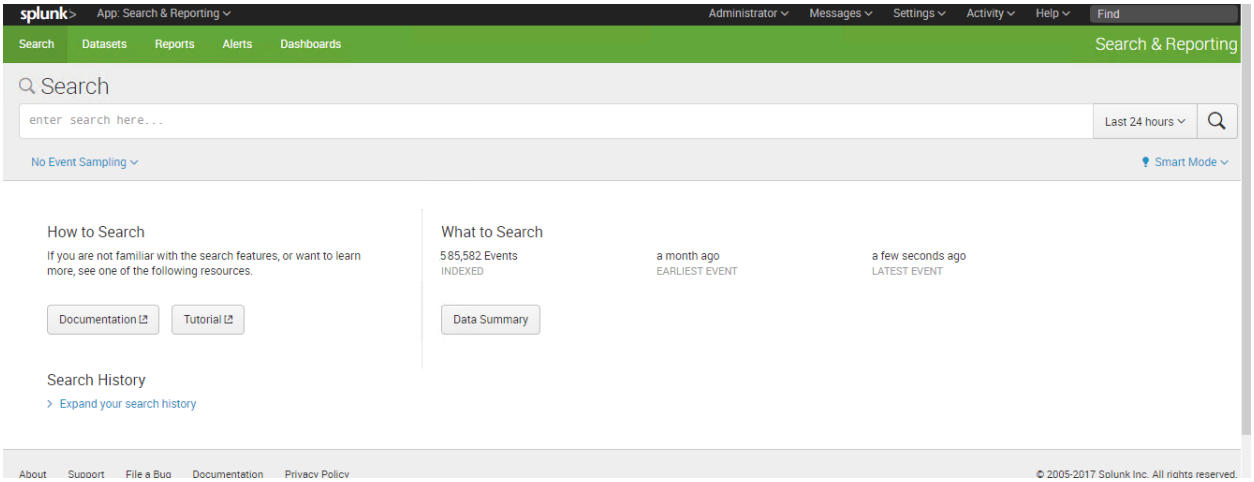
In our system Splunk server getting all windows logs from client machines automatically, for this we have installed splunk-forwarder using chef automate in every windows server. To view the logs in splunk server.

1. Enter **splunkIpAddress** in web browser and Login to the splunk server using **splunkIPAddress** and **splunkWebUIUsername** provided in the outputs section and

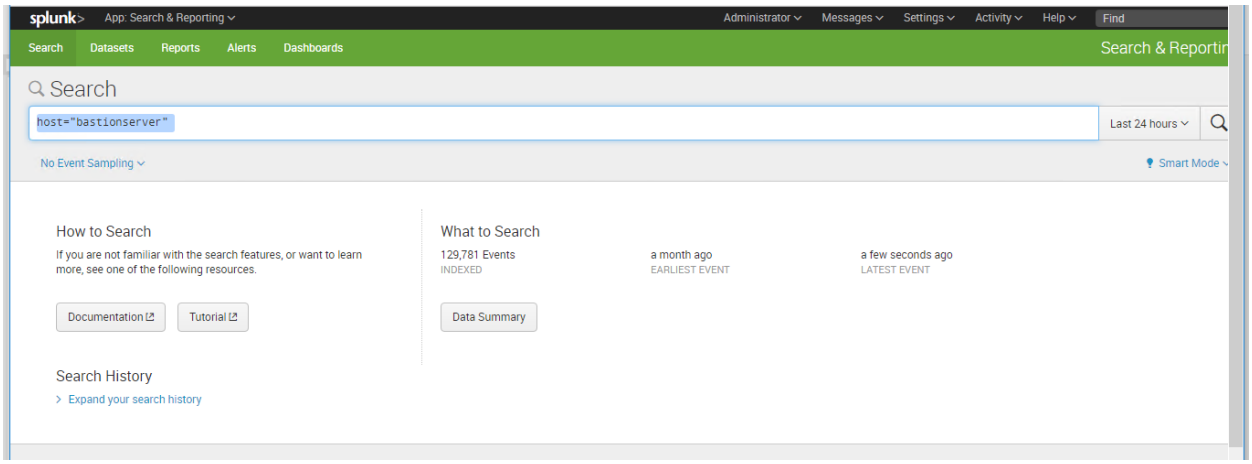
adminPassword used during template deployment**.**

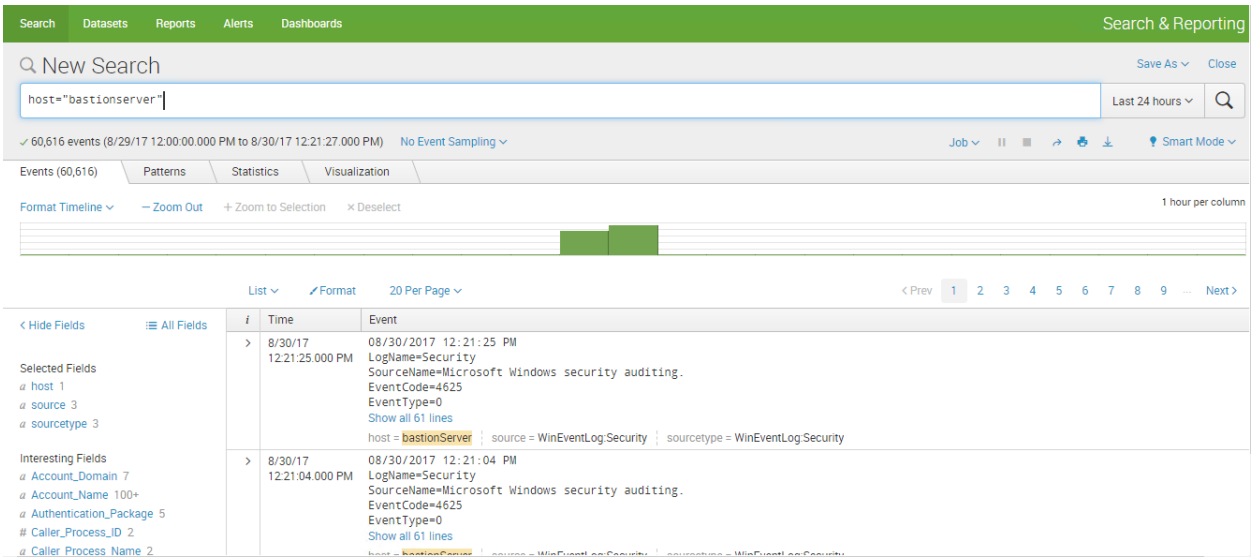


Click on **search & Reporting** on left panel of the page



On Search box enter **host="bastionserver"** and pressto check the bastion server logs.



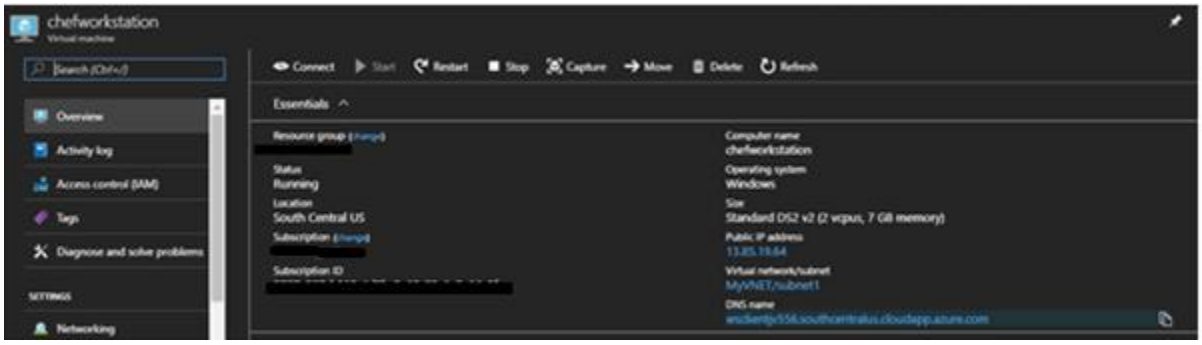


Similarly, we can view the all logs in Splunk server by searching with regular expression in search box.

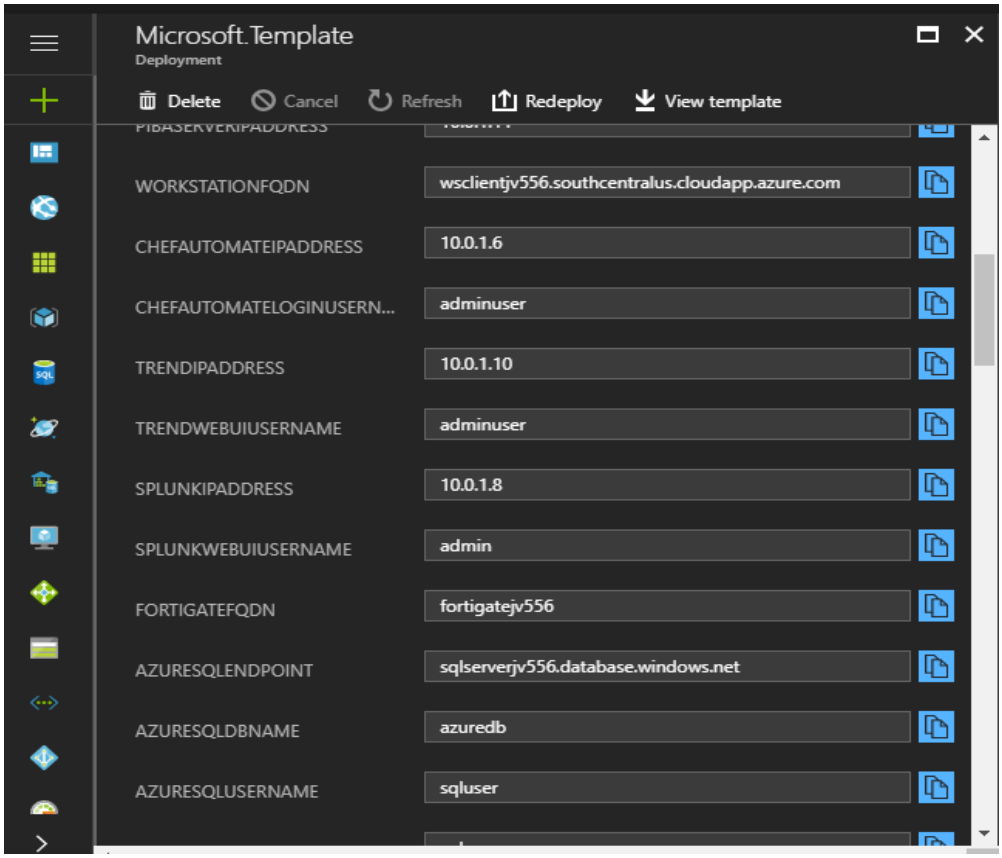
7.4. TrendMicro

Once the IOT Arm template get deploys, it will install the TrendMicro Agent on all available nodes.

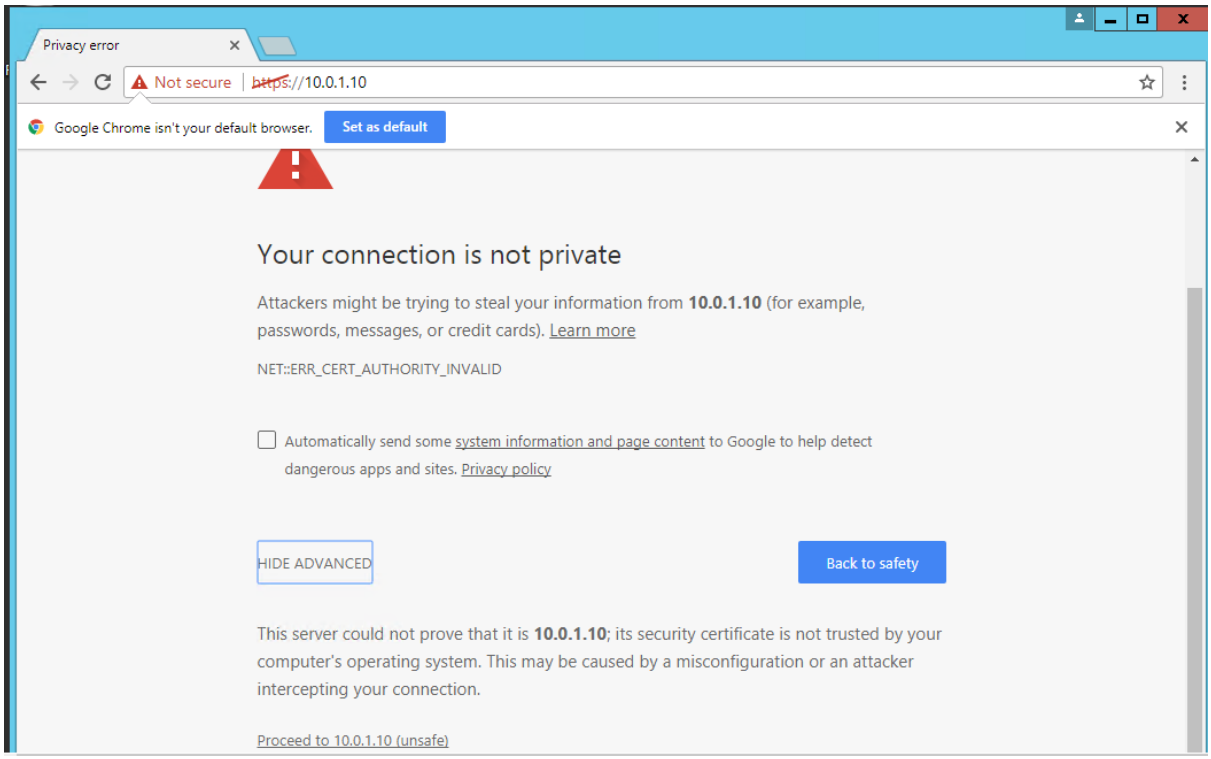
Login to Bastion Host or ChefWorkstation server.



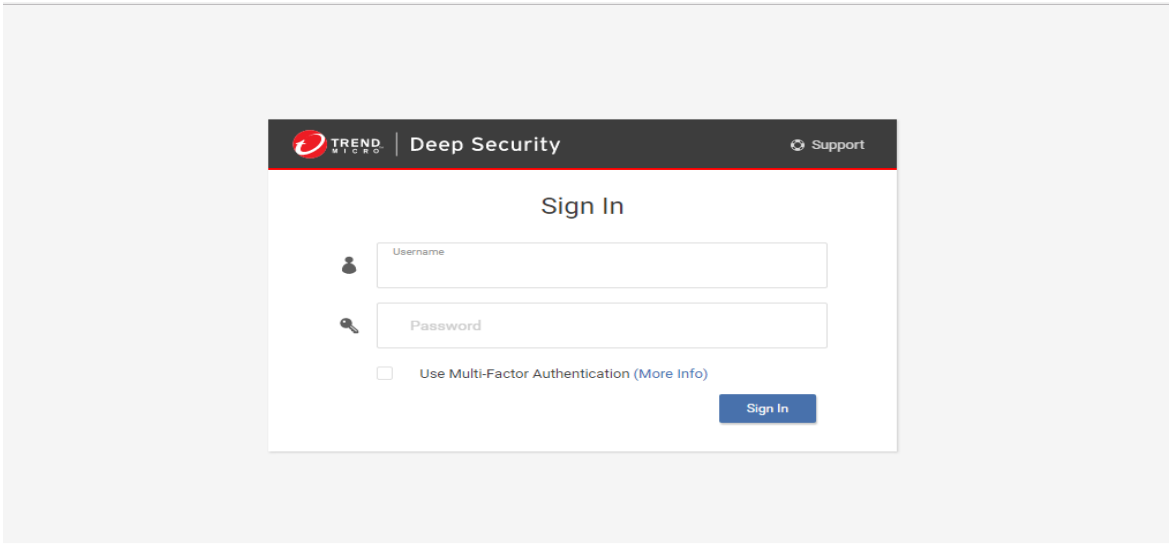
Once login open Browser and enter the TrendMicro IP address, which we get from output section of IOT ARM Template.



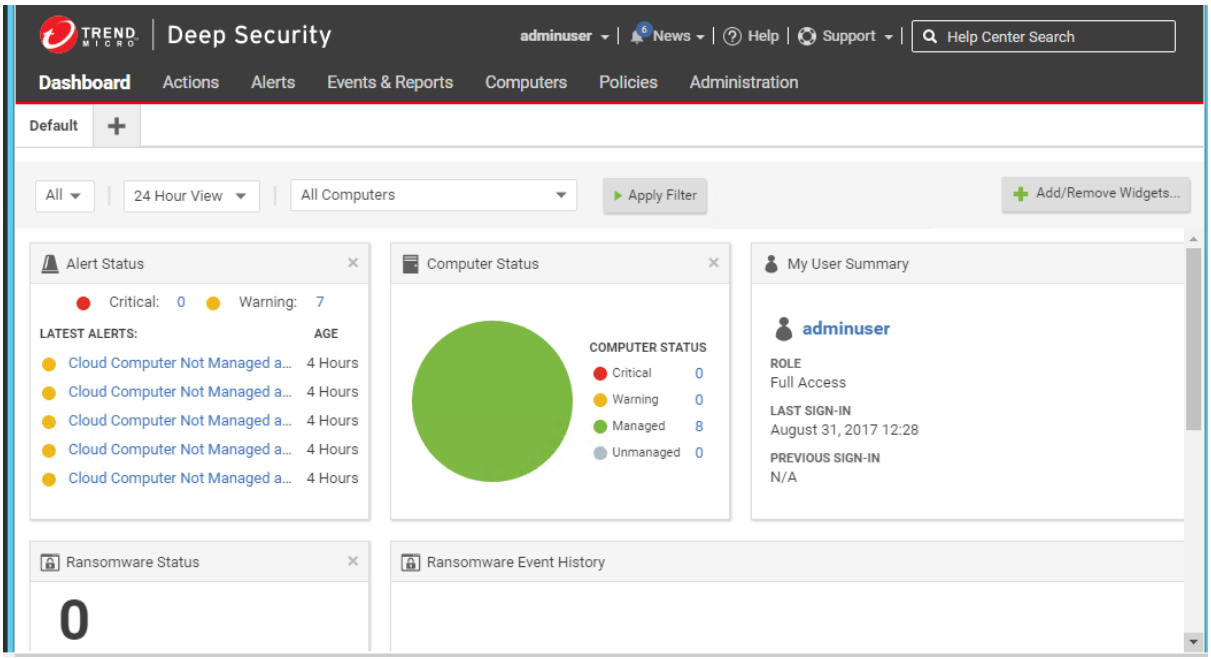
Click on “HIDE ADVANCED” and then click on “proceed to <ip>



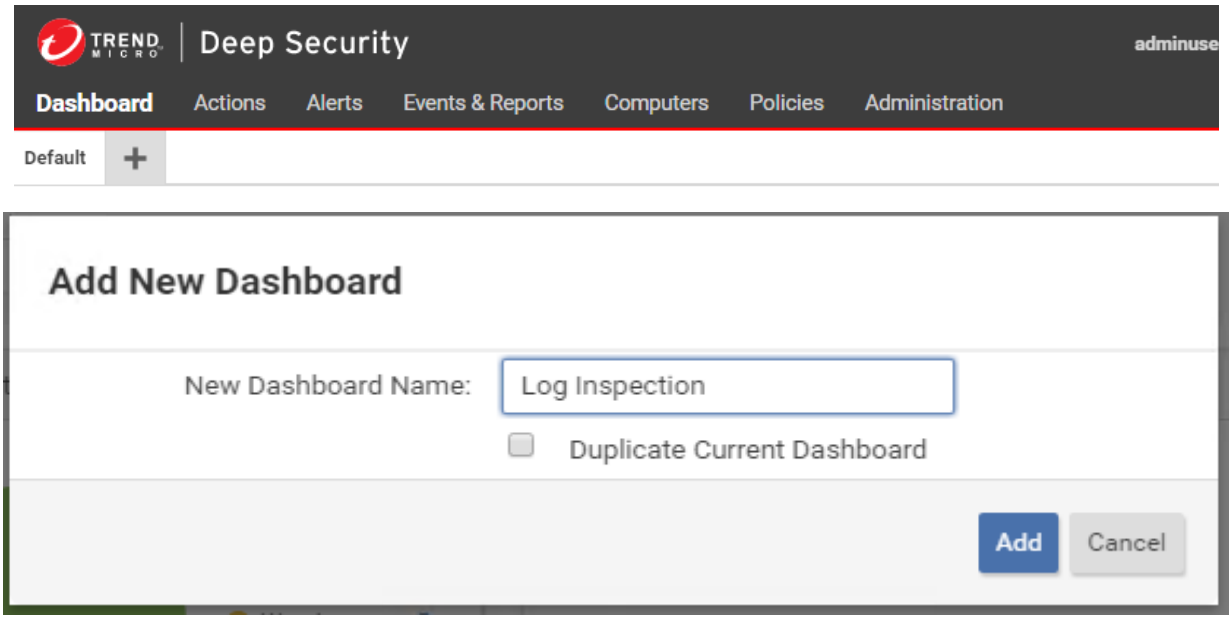
Login to Trend using the **trendWebUIUsername** provided in the output section and the **adminpassword** used while entering the details in parameter section to deploy an arm template.



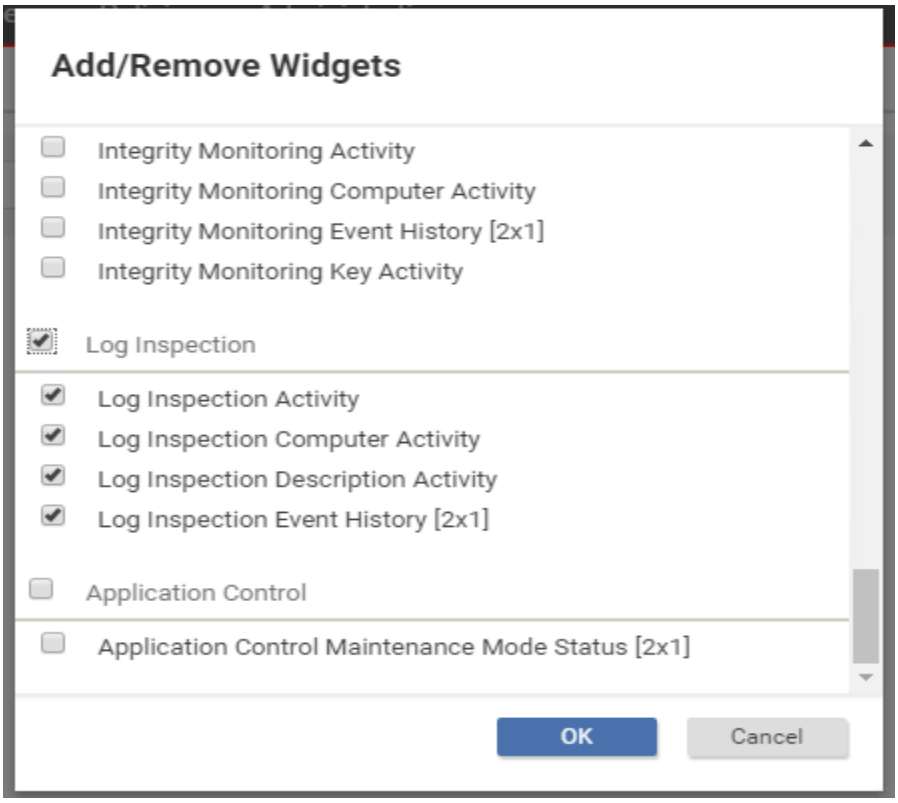
Once you logged in the below screen will appear which have default Dashboard and it lists the Alert Status, Computer Status , User Summary and Sign-in History.



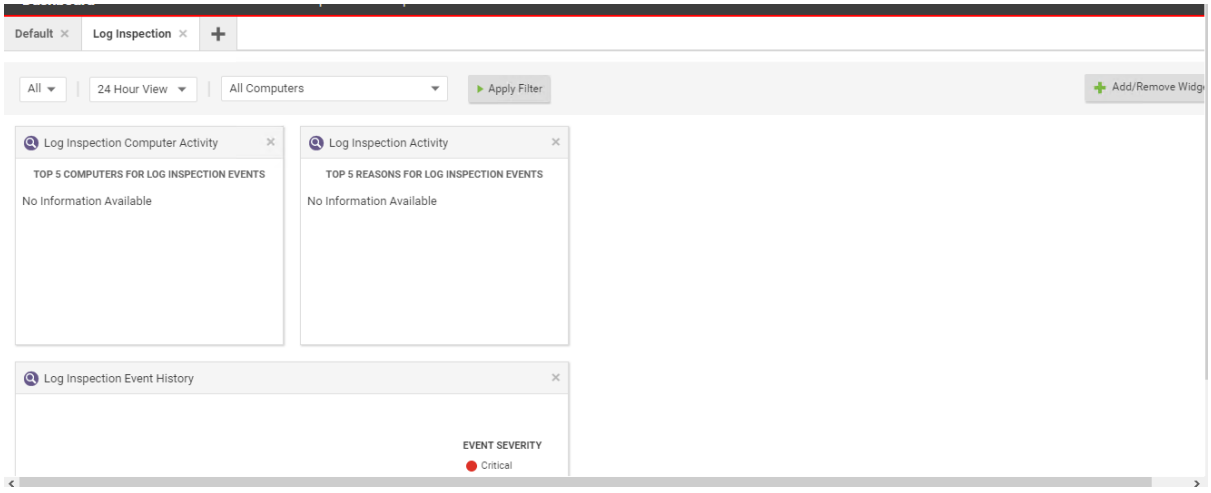
We can create our own Dashboard by clicking on "+" icon Besides Default and add the Widgets which you want to monitor.



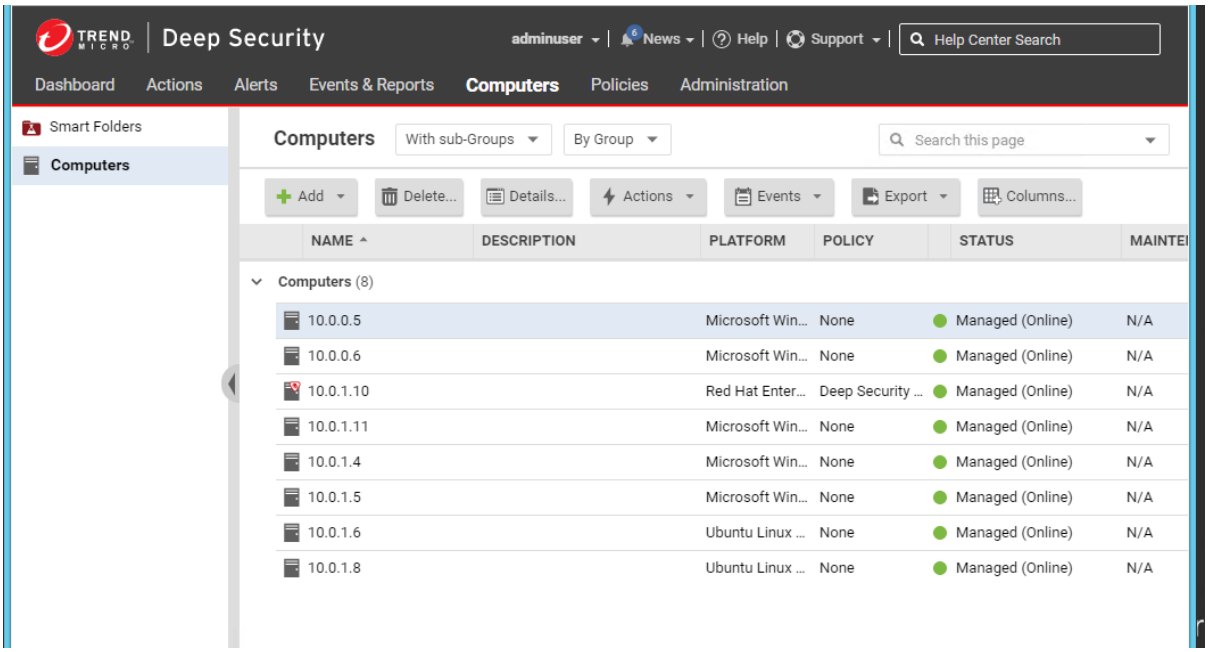
Click on Add/Remove Widgets and select **Log Inspection** and click ok



Below screen will appear with the widgets of **Log Inspection**

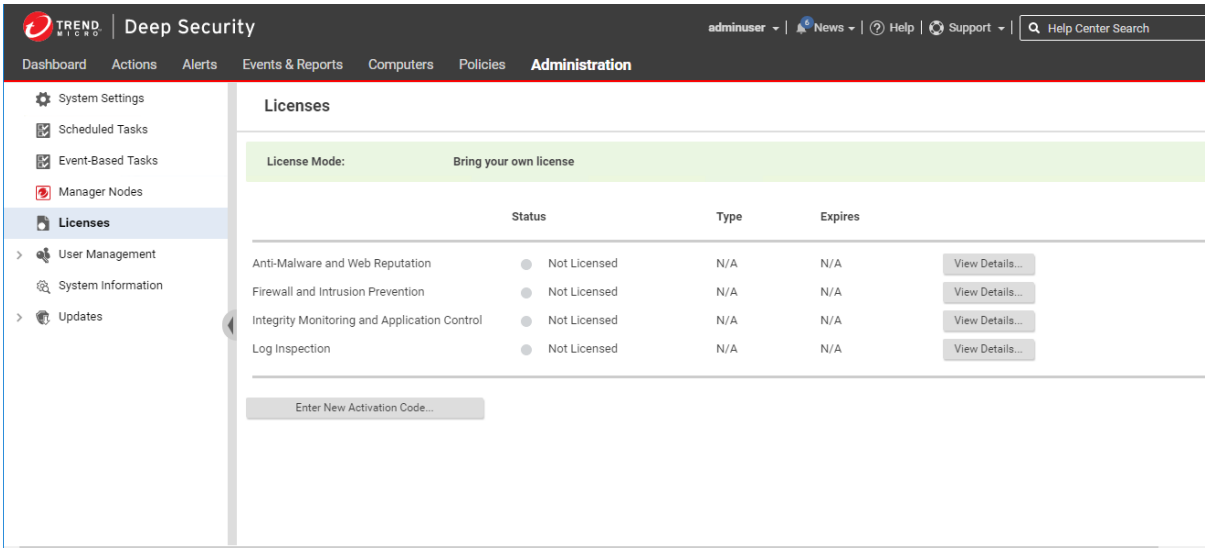


To view the nodes on which the Trend Agent got installed, click on “Computers” from top menu.

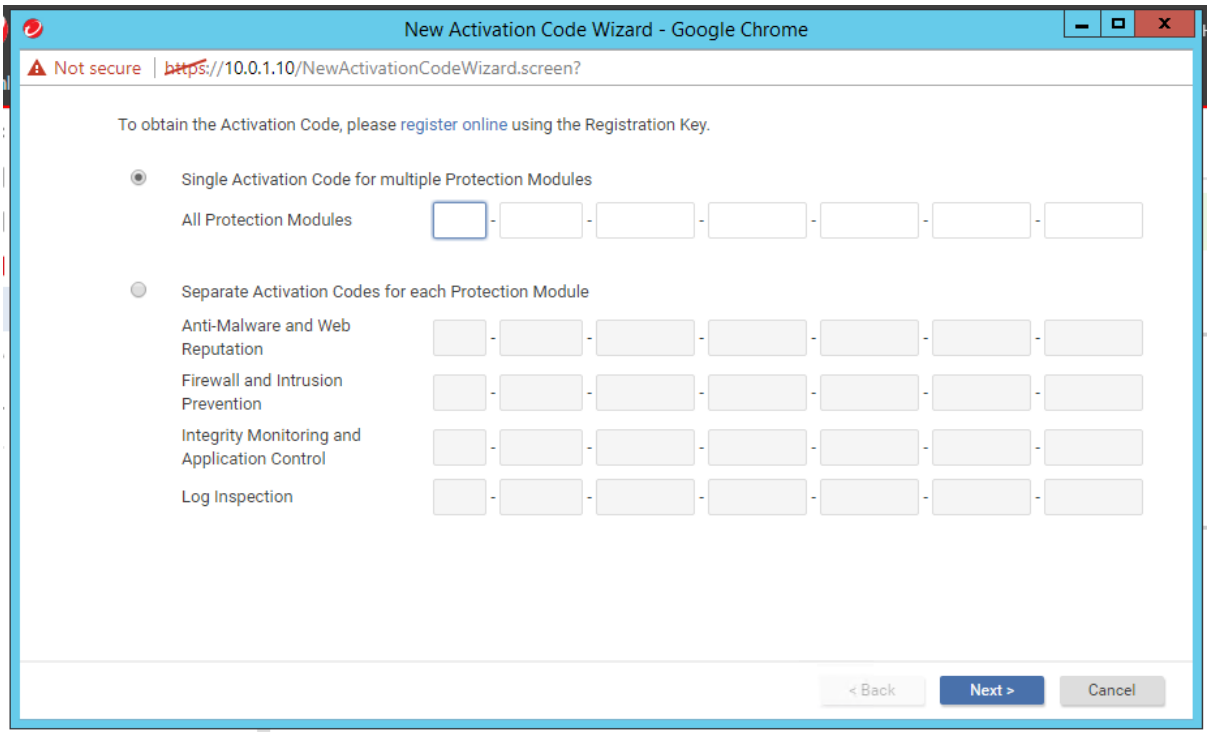


For installing the TrendMicro License, click on **Administration** from top menu.

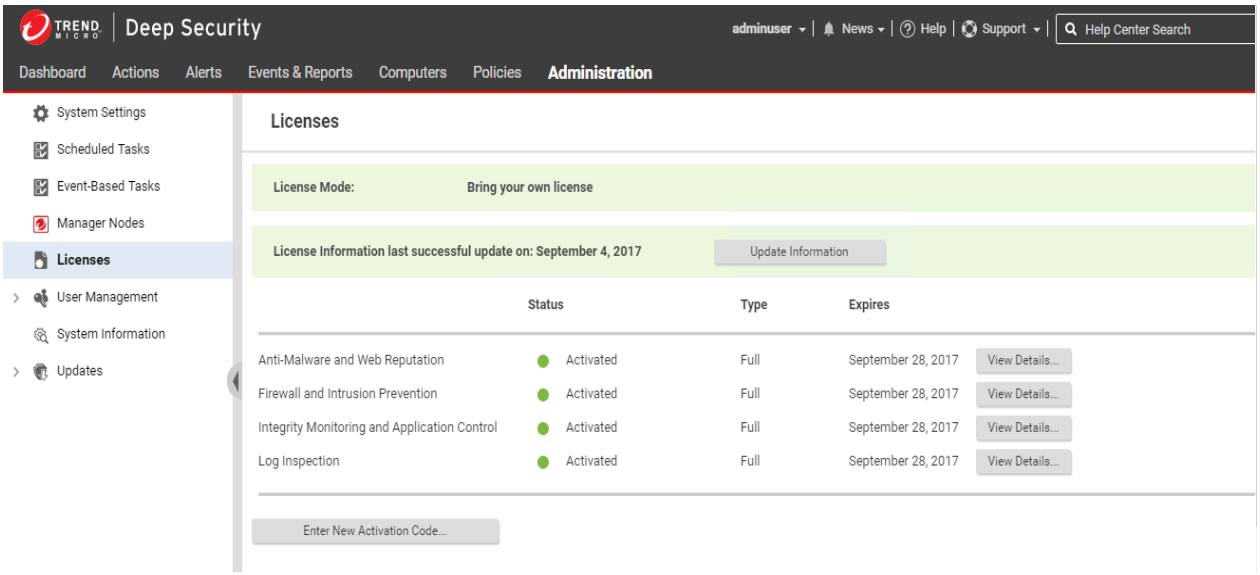
Click on **Licenses** from left side menu and then Click on **Enter New Activation Code**



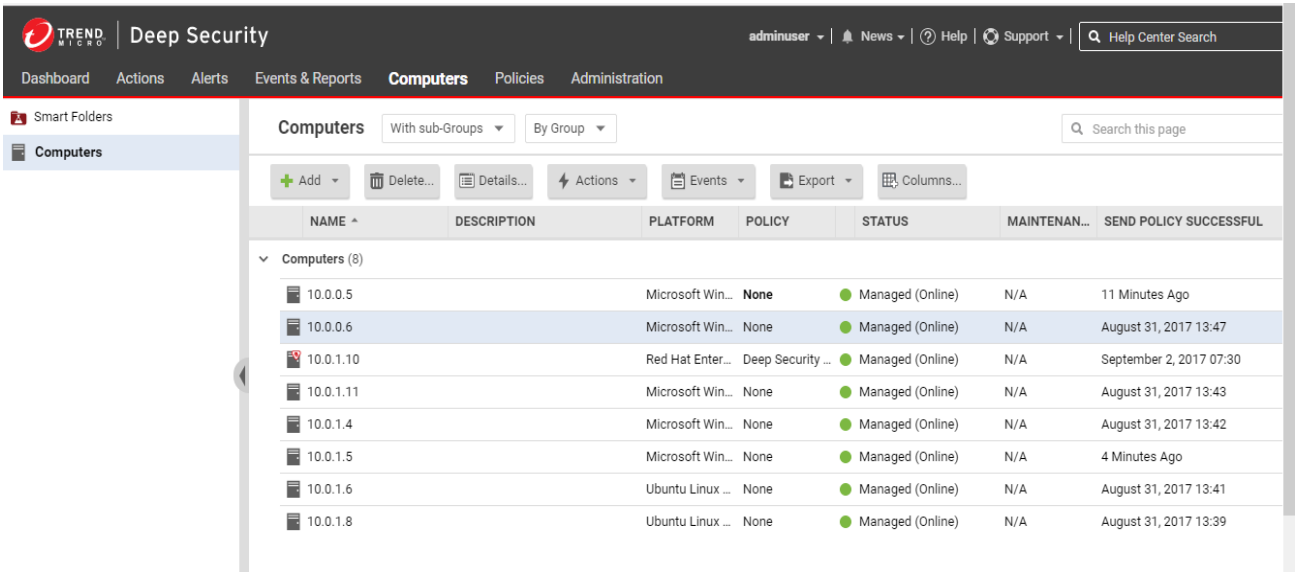
Enter the License by checking "**Single Activation Code for multiple Protection Modules"**



Once the License gets installed you will see the status to **Activated.**

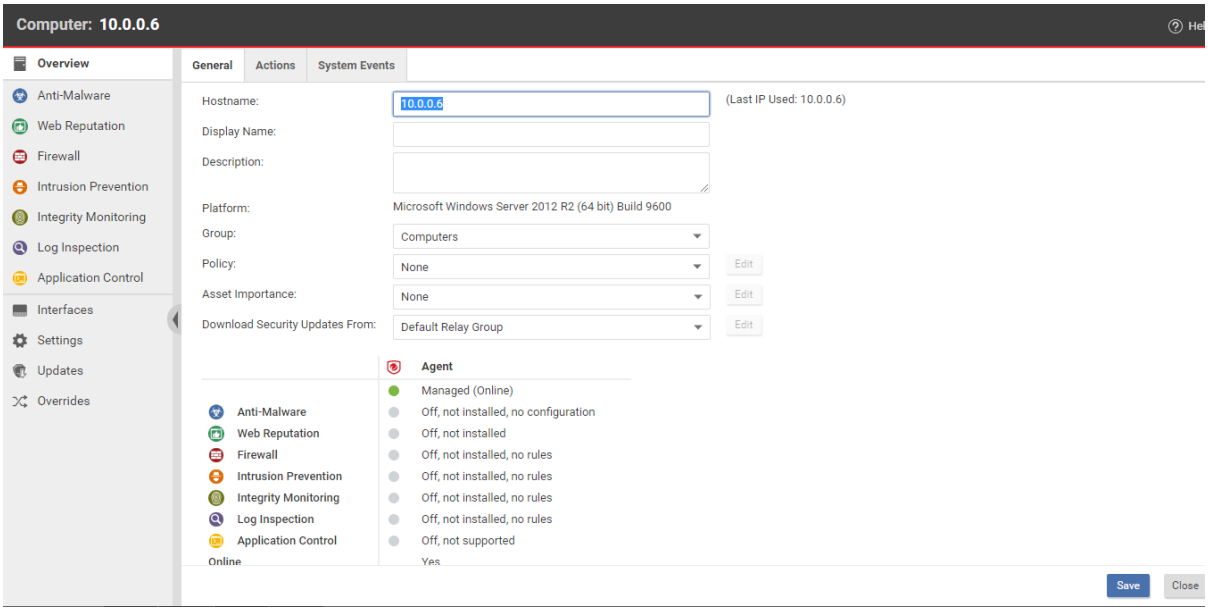


To scan available nodes, Click on "Computers" and Double click on any node. Here we are scan for malware on **ChefWorkStation** so clicking on **10.0.0.6**



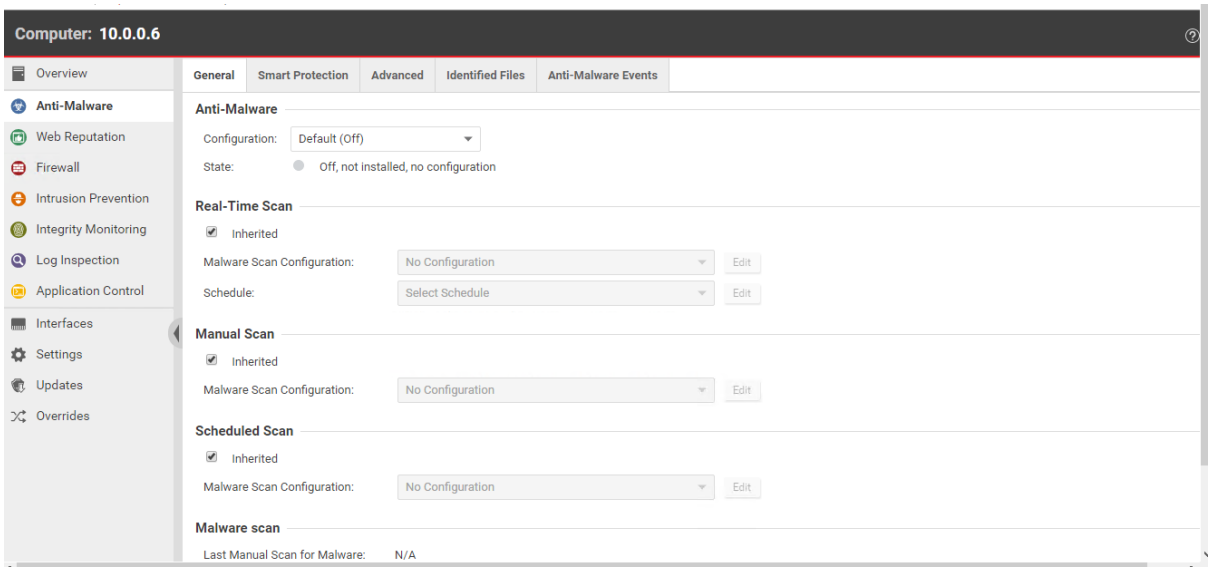
The below screen will appear, you can see Anti-Malware is **Disabled**.

Click on Anti-Malware from left side menu.



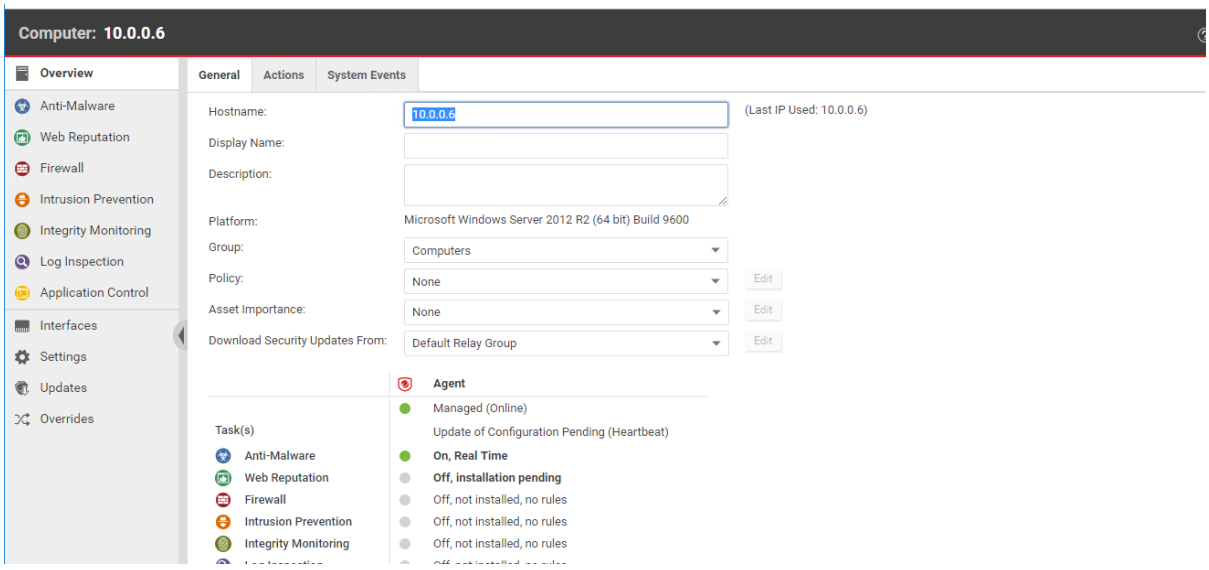
Select On from the dropdown menu of configuration and uncheck the inherited under Real-Time Scan, Manual Scan and Schedule Scan.

Once the changes made click on Save from bottom of the page.



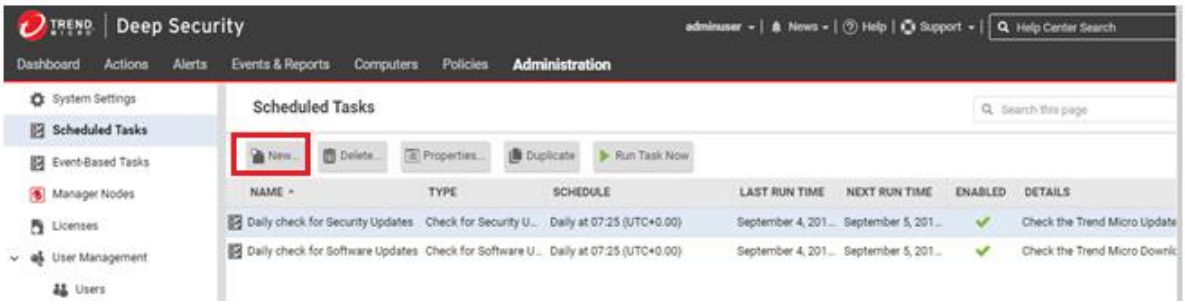
Once the changes saved, Click on Overview to see the Anti-Malware is On and Activated.

Note: it might take some time to get Activated.

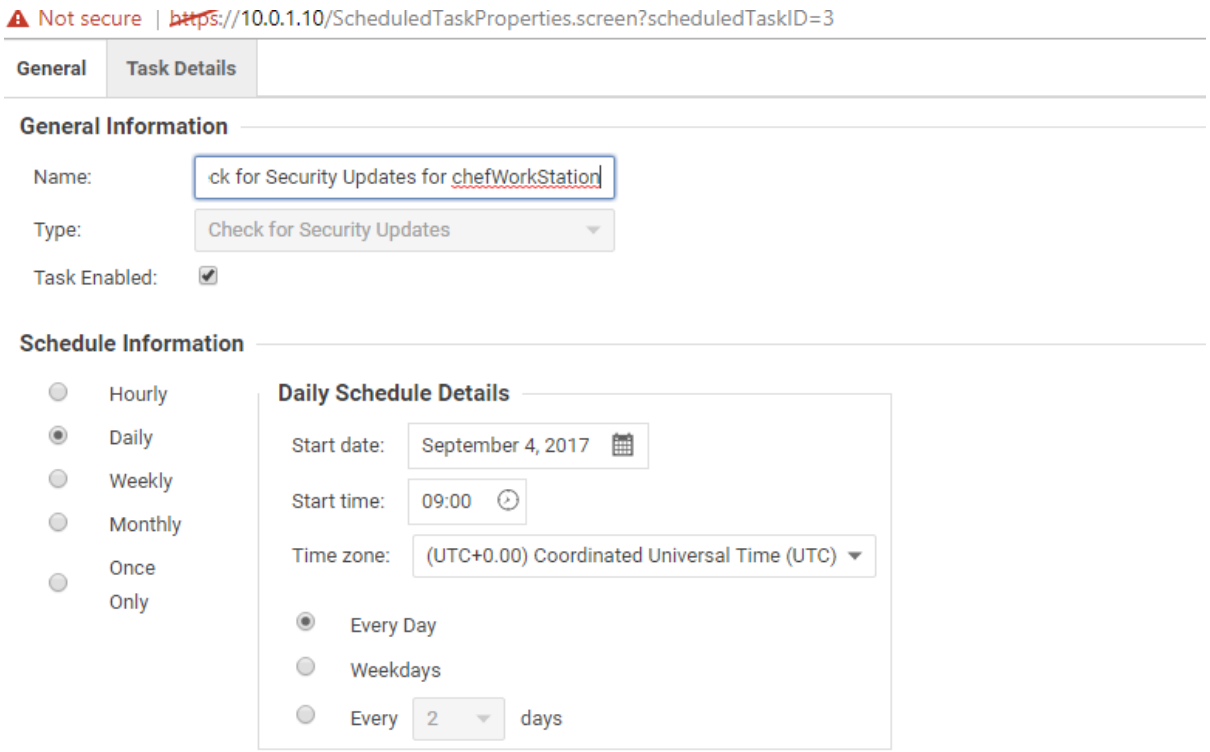


We can schedule a scan for Hourly, Daily, Weekly, Monthly, Only once.

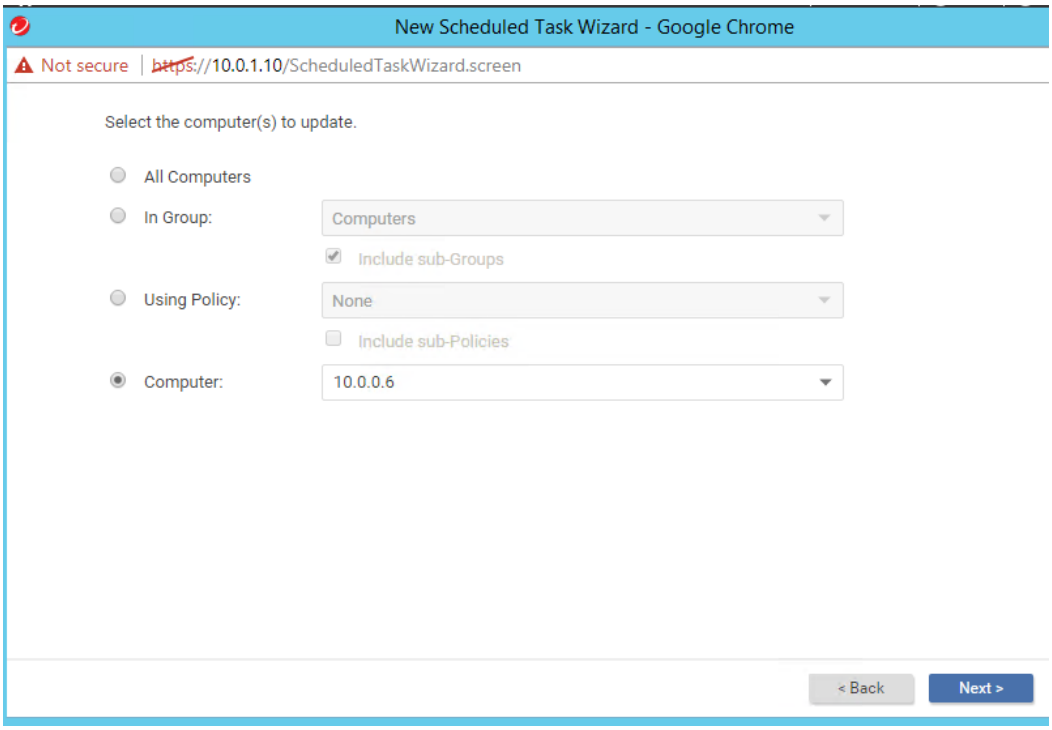
To schedule a scan, navigate to **Administration** and click on **New**.

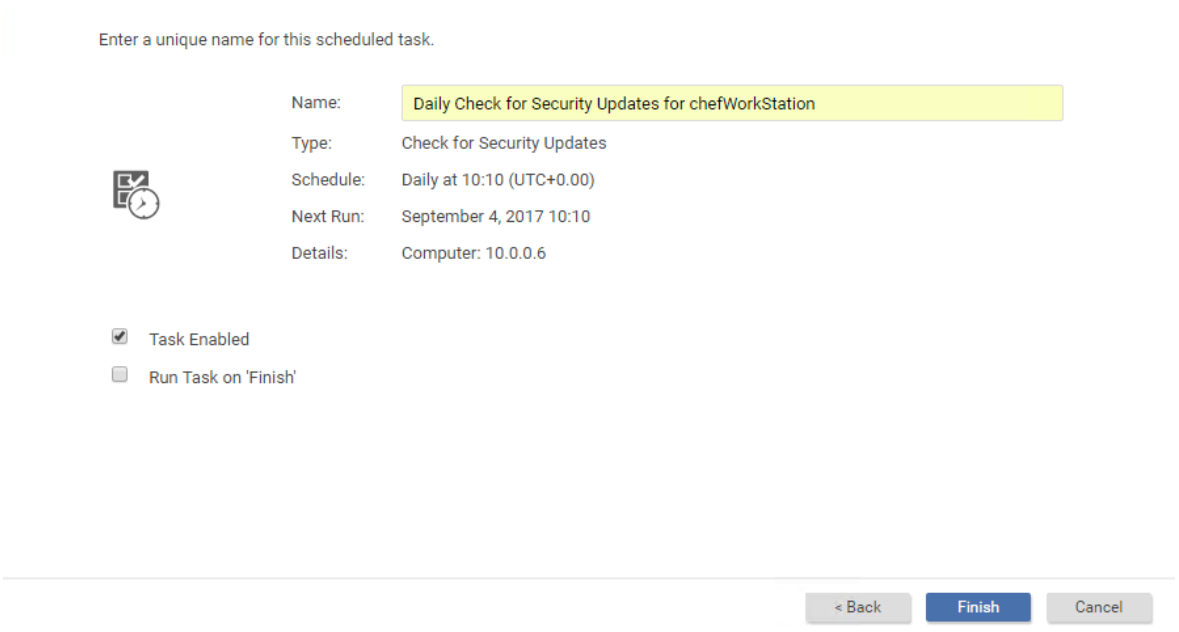


Enter the Name for the Schedule Task and in **schedule information** select Daily, start time and click on **Next**



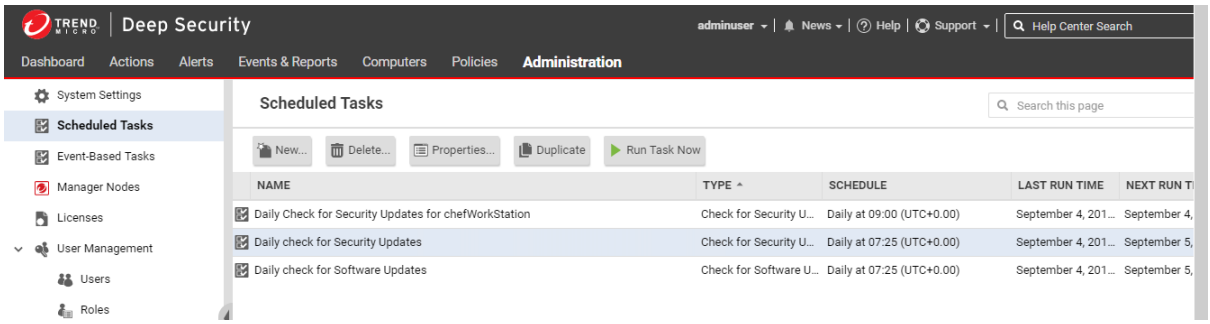
Check the Computer and from the dropdown list select ChefWorkStation Node.



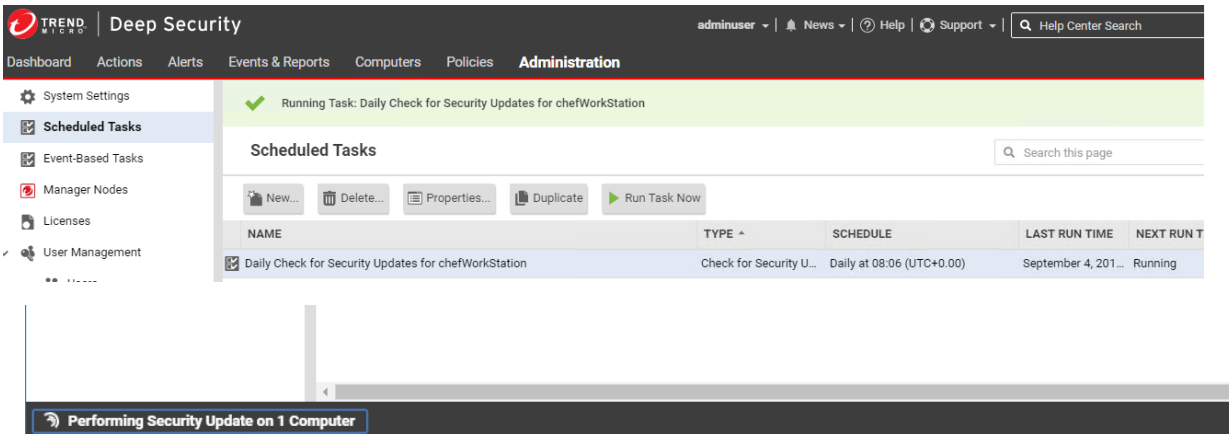


Click on Finish

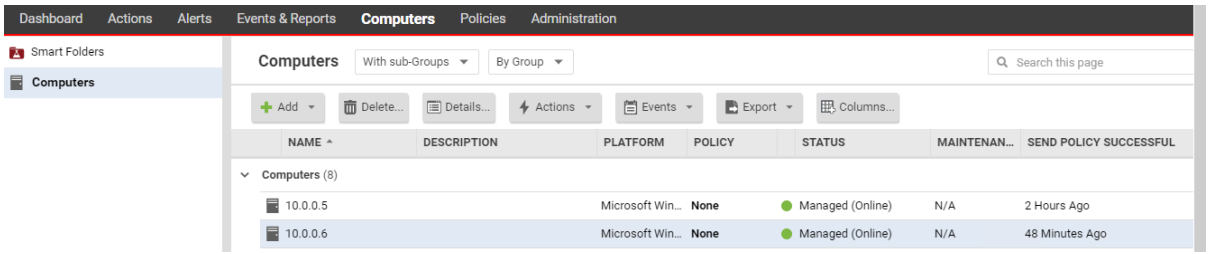
Once done, you can see the created Task under the Scheduled Task list.



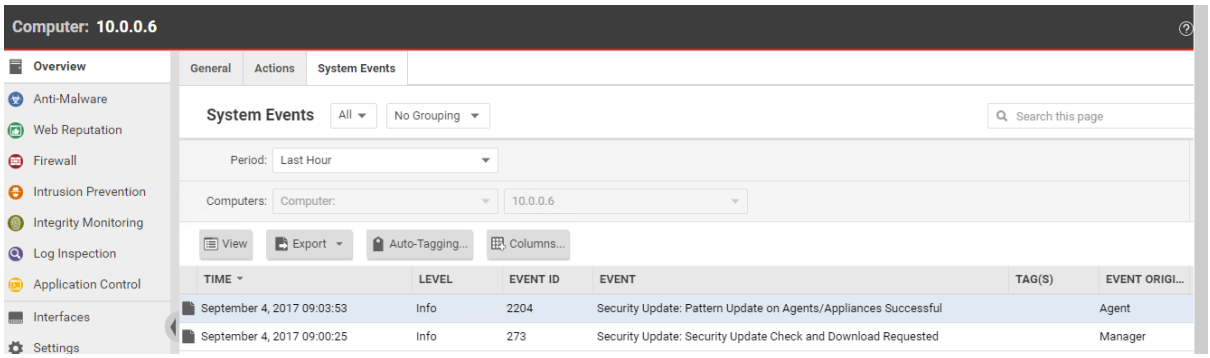
Select the Created Task and Click on Run Task Now or it will run the Scheduled task at specified time.



To view the generated report navigate to Computers and double Click on ChefWorkStation node (10.0.0.6).

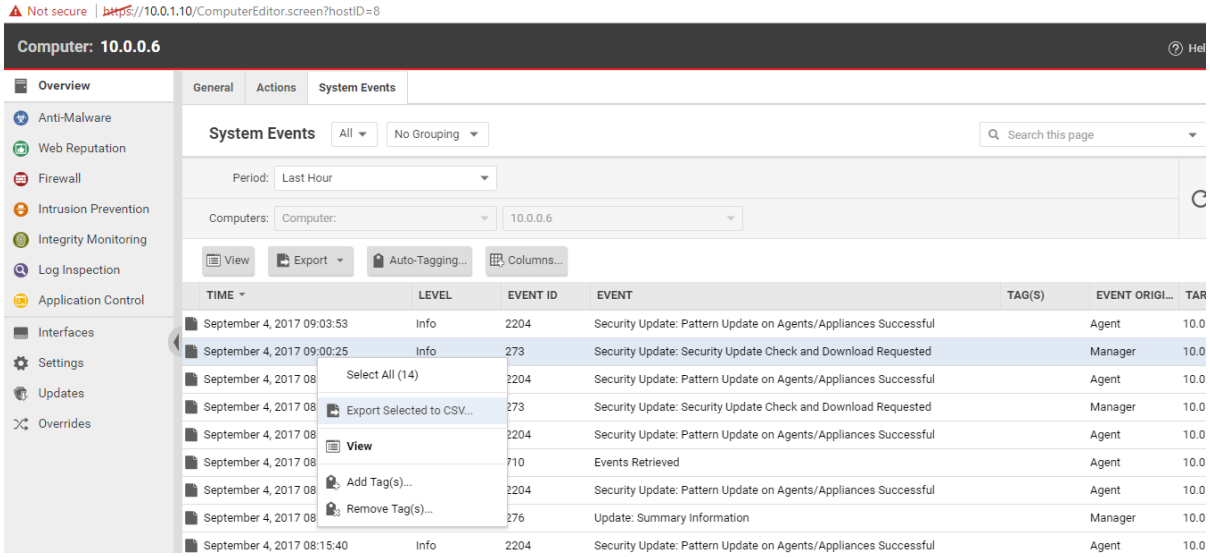


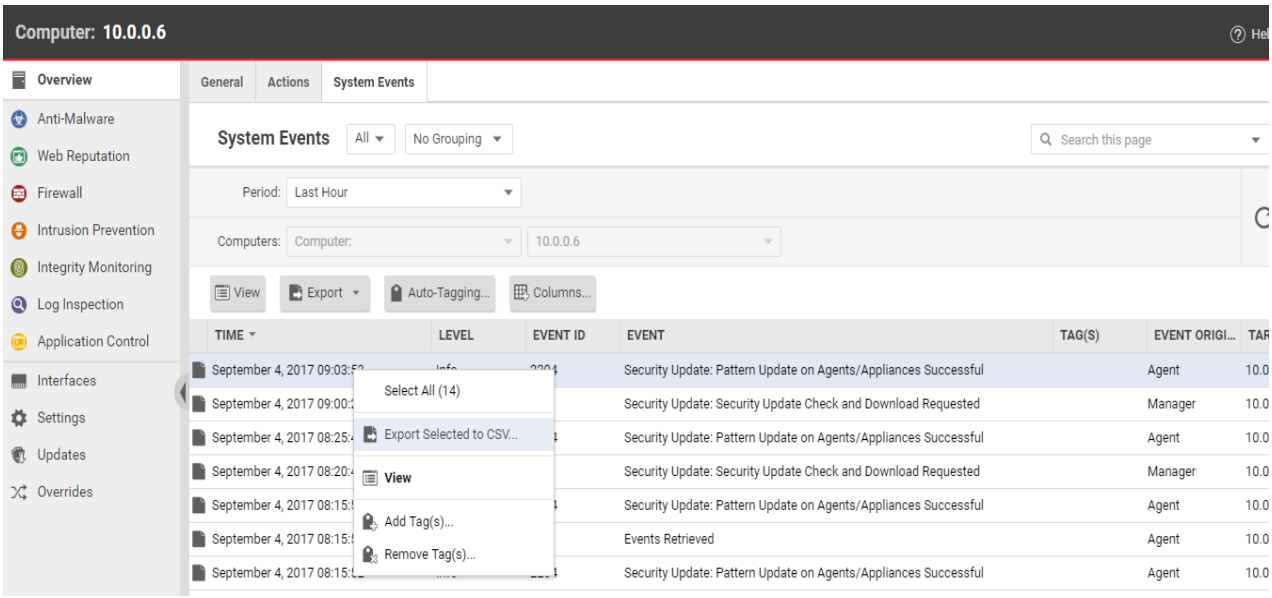
It will open below screen in new window, click on System Events from left side Overview menu



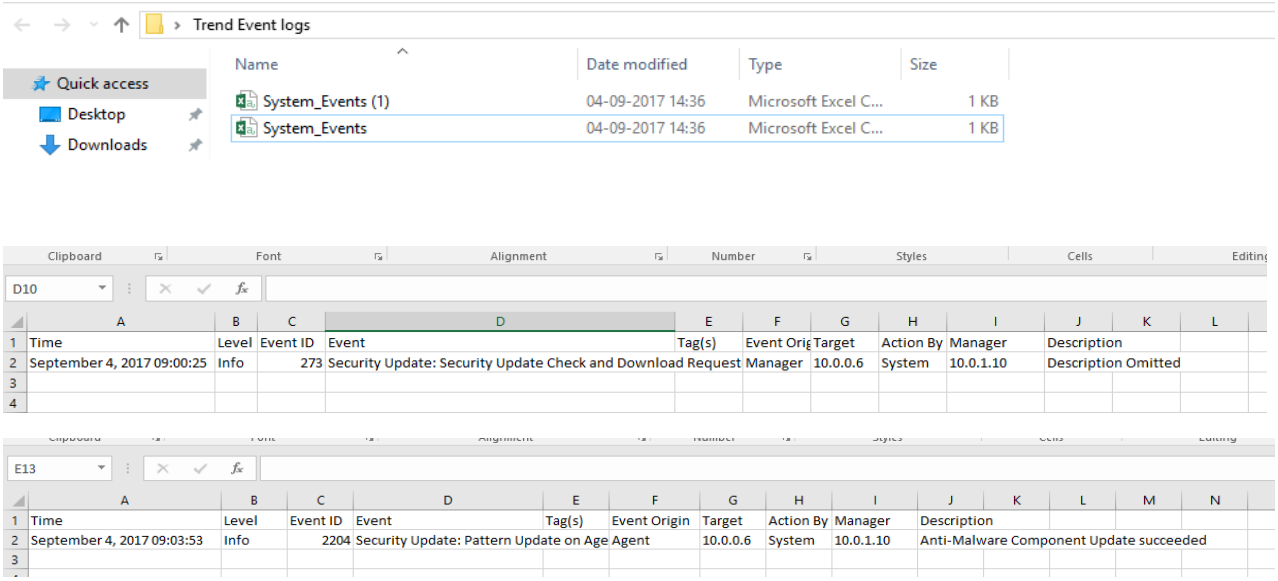
Right click on Manager report and click on Export Selected to .csv to get the manager report.

Right click on Agent report and Click on Export Selected to .csv to get the agent report.





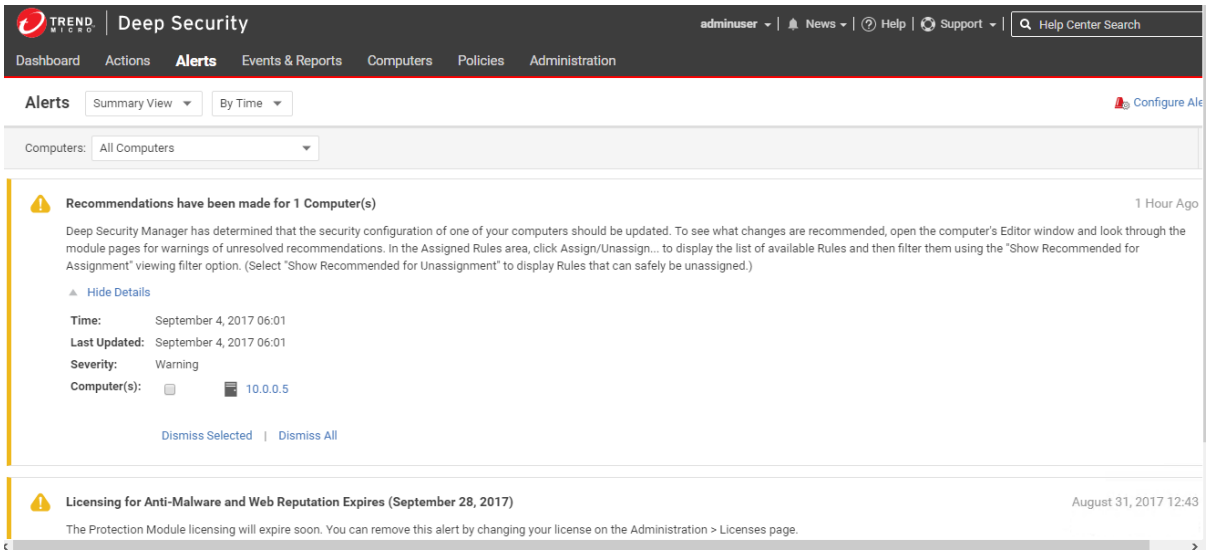
After the log files get downloaded, we can see the report of ChefWorkStation.



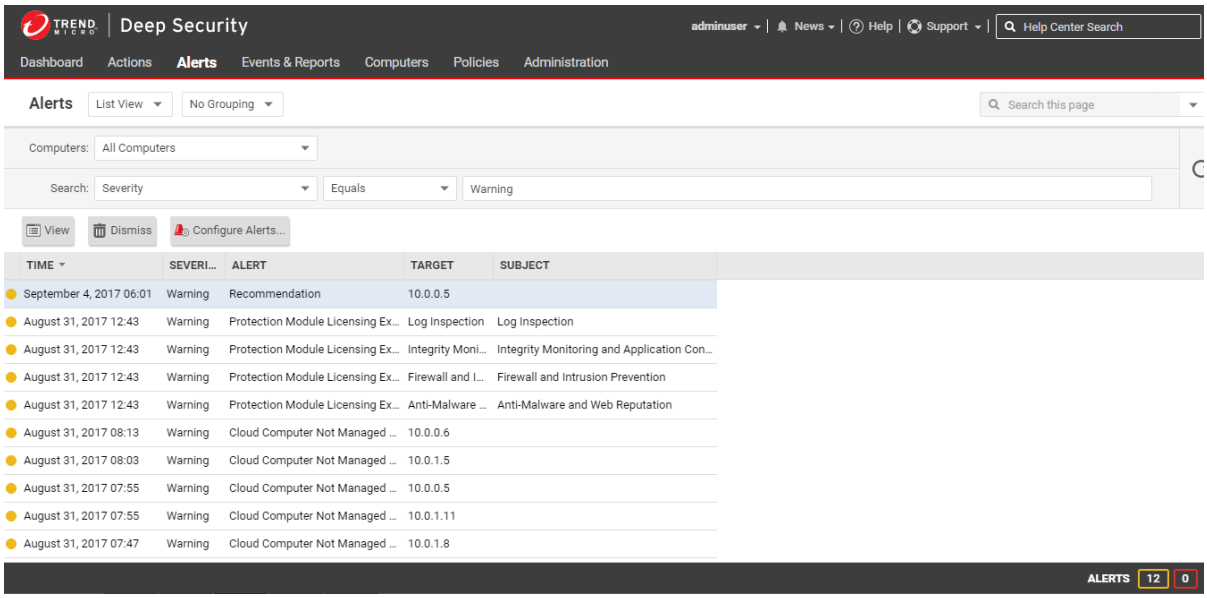
Similarly, we can Schedule task for Malware, Software Updates, Open Ports, Alert Summary on each node.

Alerts:

If any Malware detected then appropriate action is taken, logs the events and raises an alert. You can view the alerts in the Alert tab on main page.



To view the Alert List Click on Alerts from bottom of the screen, it will redirect you to alert list.



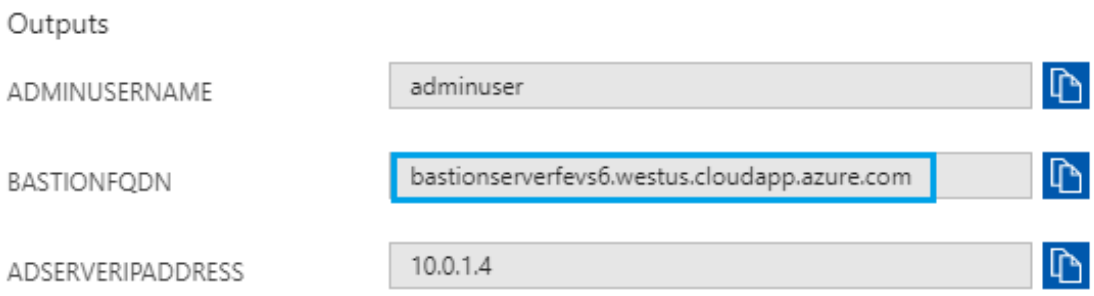
USES:

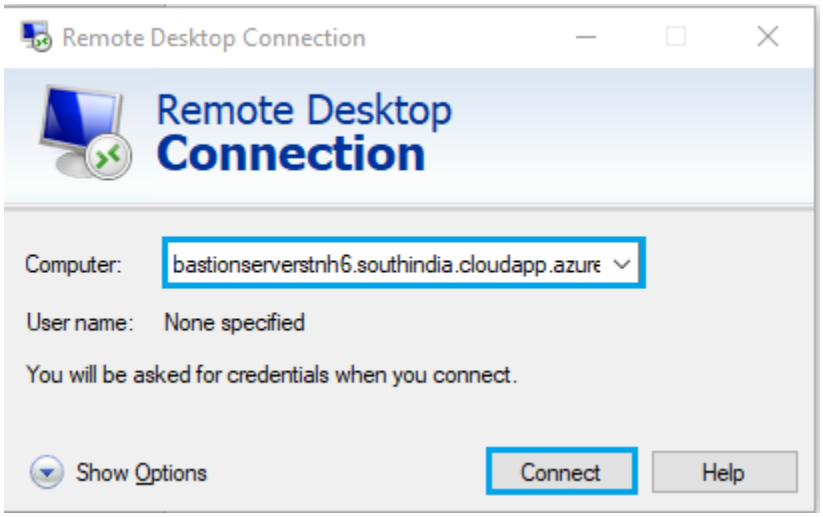
1. **Adding computer to deep security manager**
   Use the computers page of the deep security manager to discover local computers or to connect to your cloud
2. **Deploying protection**
   Deep security Agents are available for a wide variety of platforms. You can install the Agents manually or take advantage of the automation tools available for cloud provider such as deployment scripts for VM Extension for Microsoft Azure.

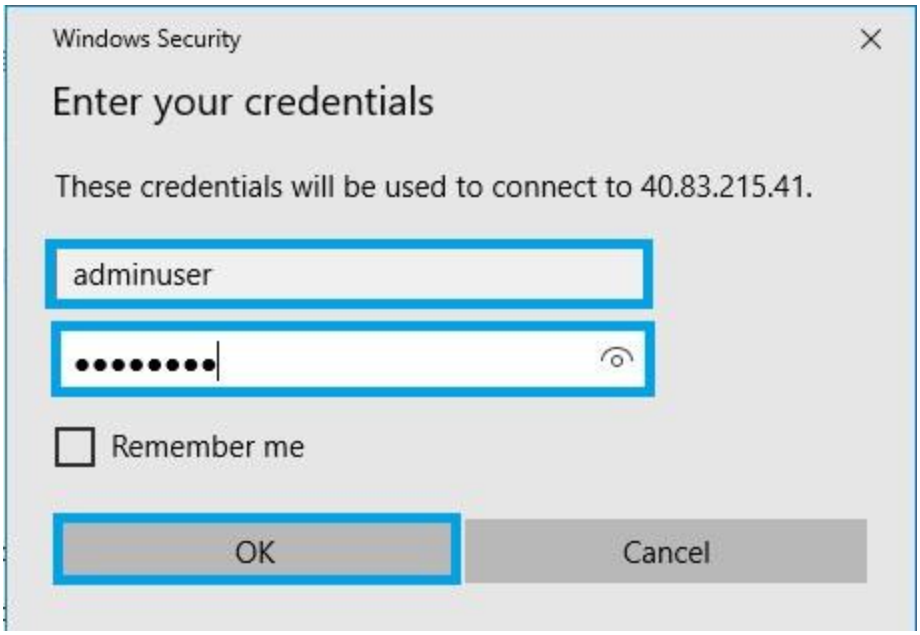
3. **Assigning security policies**
   Next, assign security policies based on the types of systems you're protecting. Deep Security comes with a collection of policies designed for a variety of platforms and purposes - you can use these policies or create your own.
4. **Keeping your protection up to date**
   The Trend Micro Smart Protection network updates the protection modules on your computers as soon as new threats are identified**.**
5. **Keeping informed of Deep security events**
   Use the customizable dashboard for quick, at-a-glance, views of the status of your Deep security system. Create scheduled Tasks to periodically send out customizable reports and set up your user account to receive notifications by email of important alerts

8. Create User for PI Business Analytics (PIBA) Interface

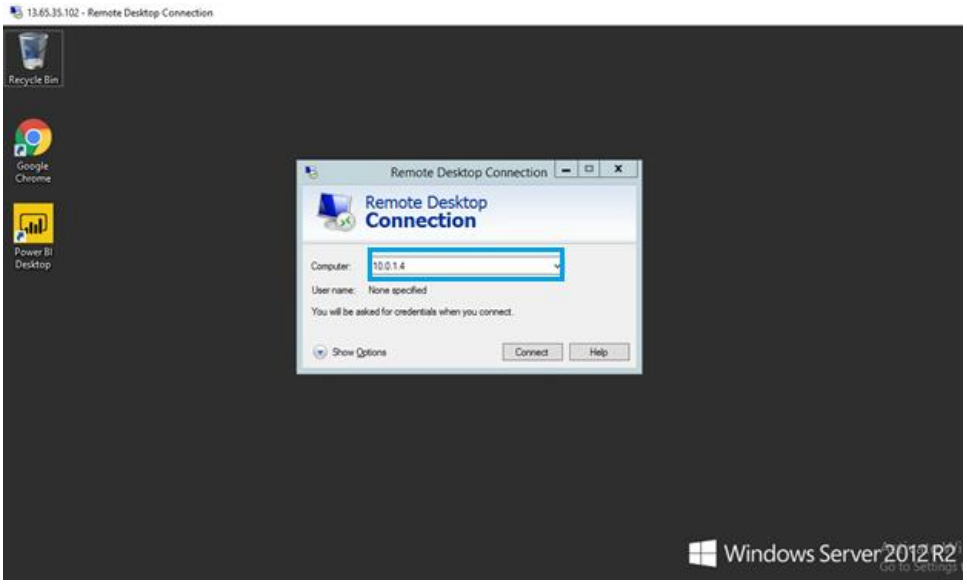
1. Login to the **Bastion Host VM** using **BASTIONFQDN** and **ADMINUSERNAME** provided in the **Outputs** section



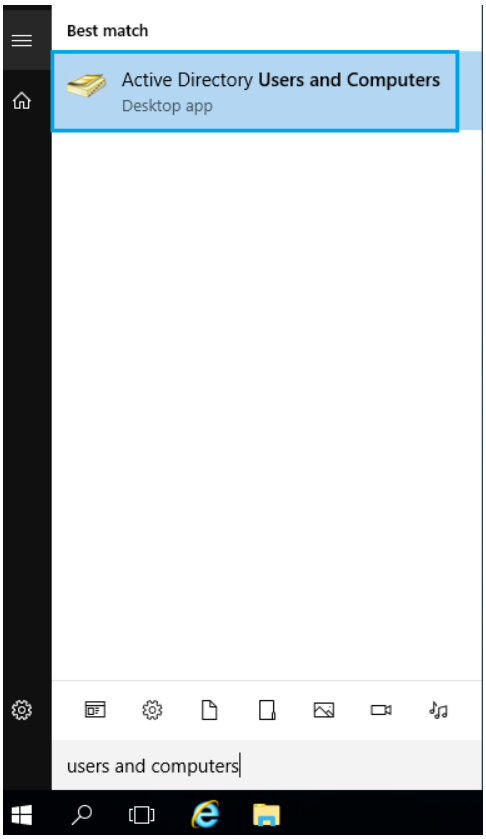




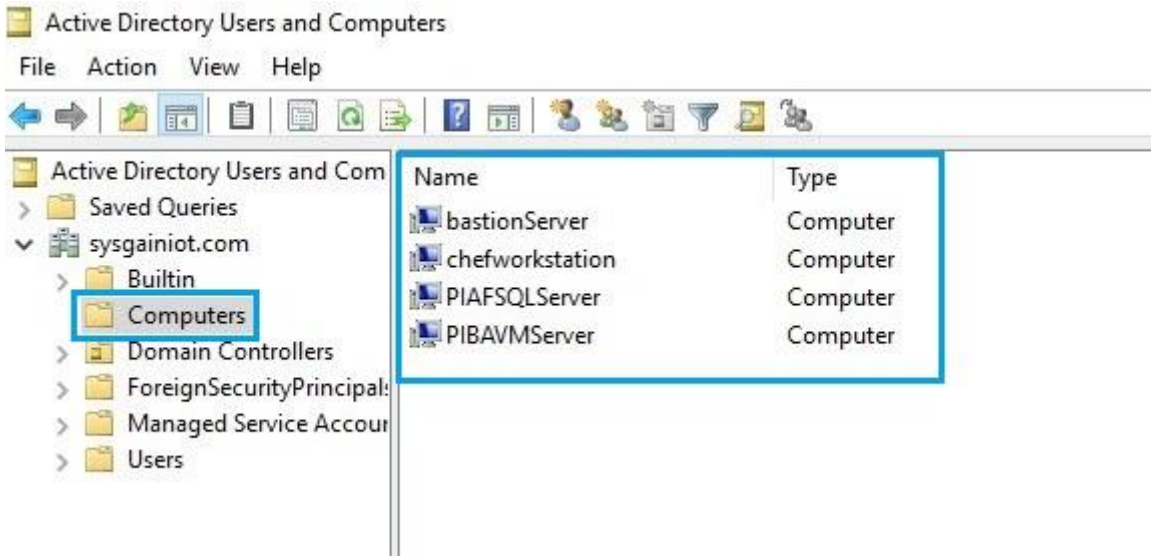
2. From the Bastion host, connect to **the Active Directory Virtual Machine** through the private address with the credentials provided in the **output** section.



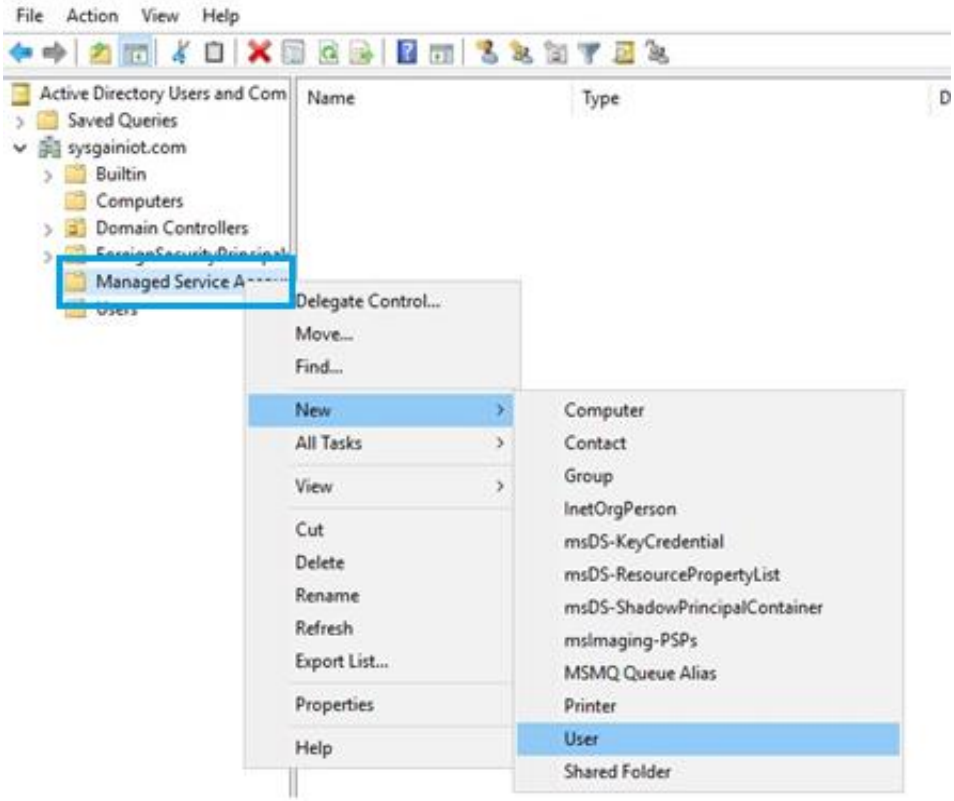
3. From the Start menu, select **Active Directory Users and Computers**.



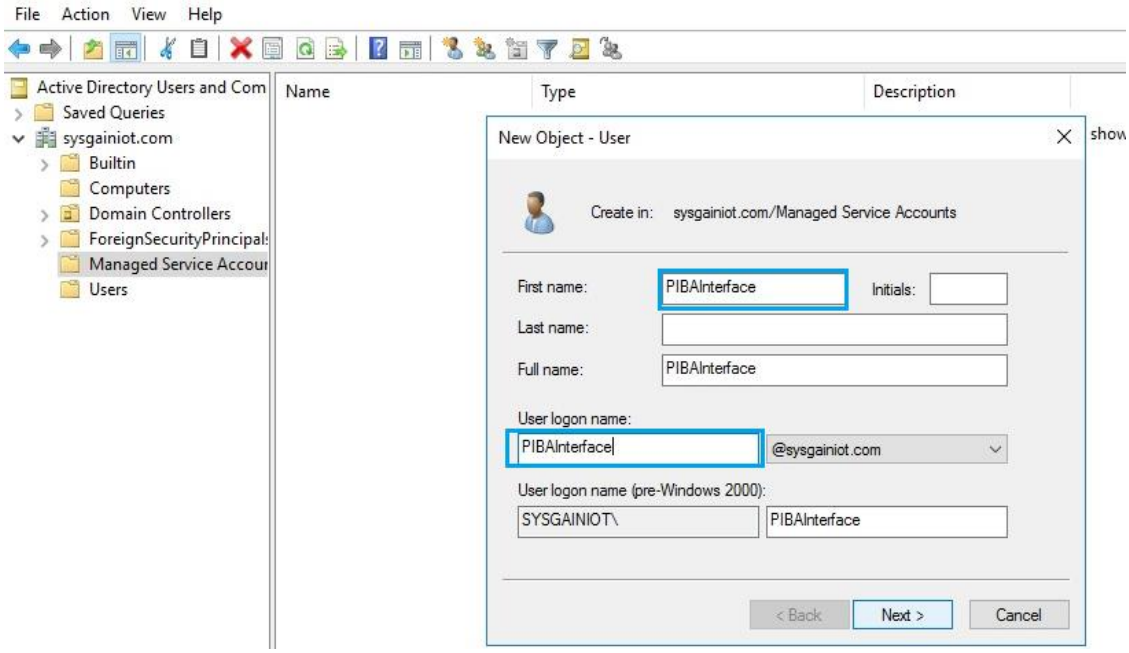
4. Click on domain name which you created. Select **Computers** to see the list of virtual machines added to the active directory. The following Virtual Machines that are added into the Active Directory are:
    - Bastion server
    - Chef workstation
    - PIAF SQL Server
    - PIBA VM Server
    - PIDA VM Server



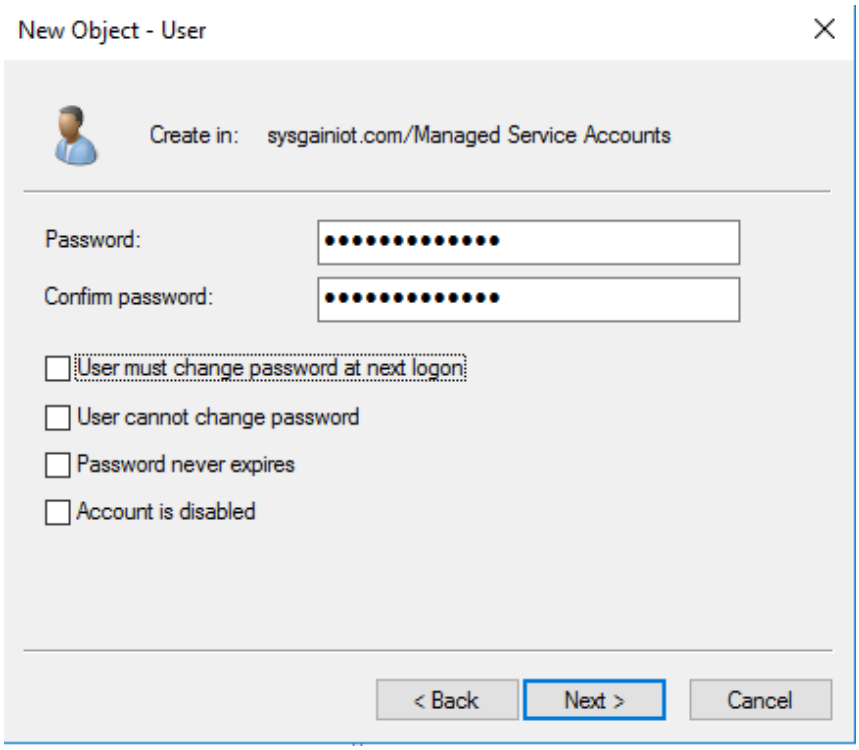
5. Right click on **Managed Service Account > New > User**.



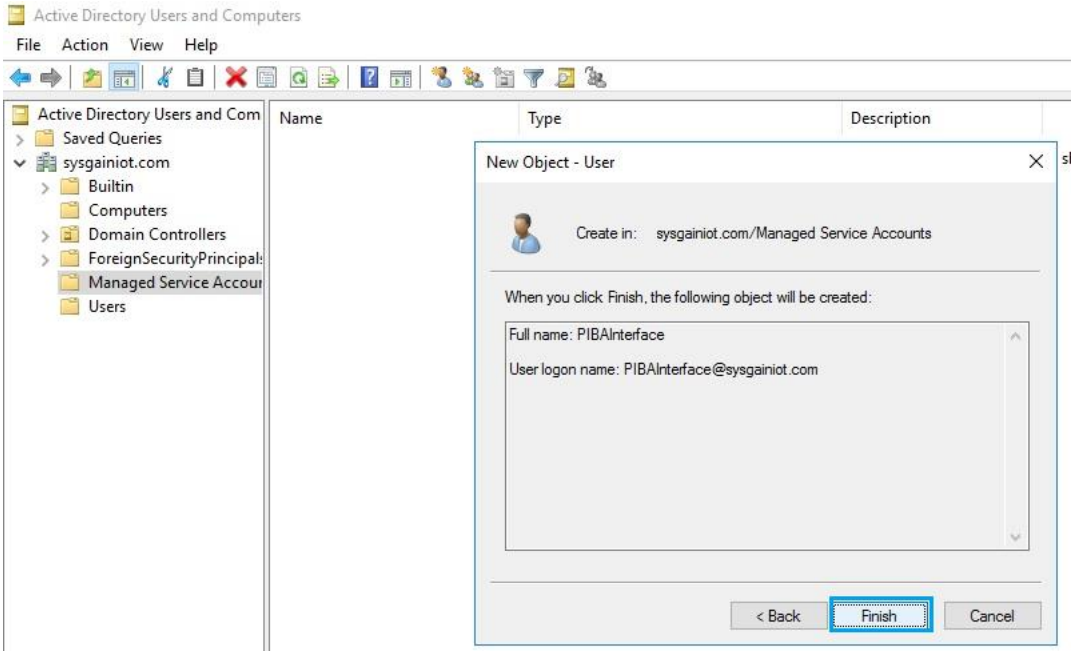
6. To create the user for PIBA, enter the **First name** and **User logon name** as **PIBAInterface** .Make sure both are same. Click on **Next**.



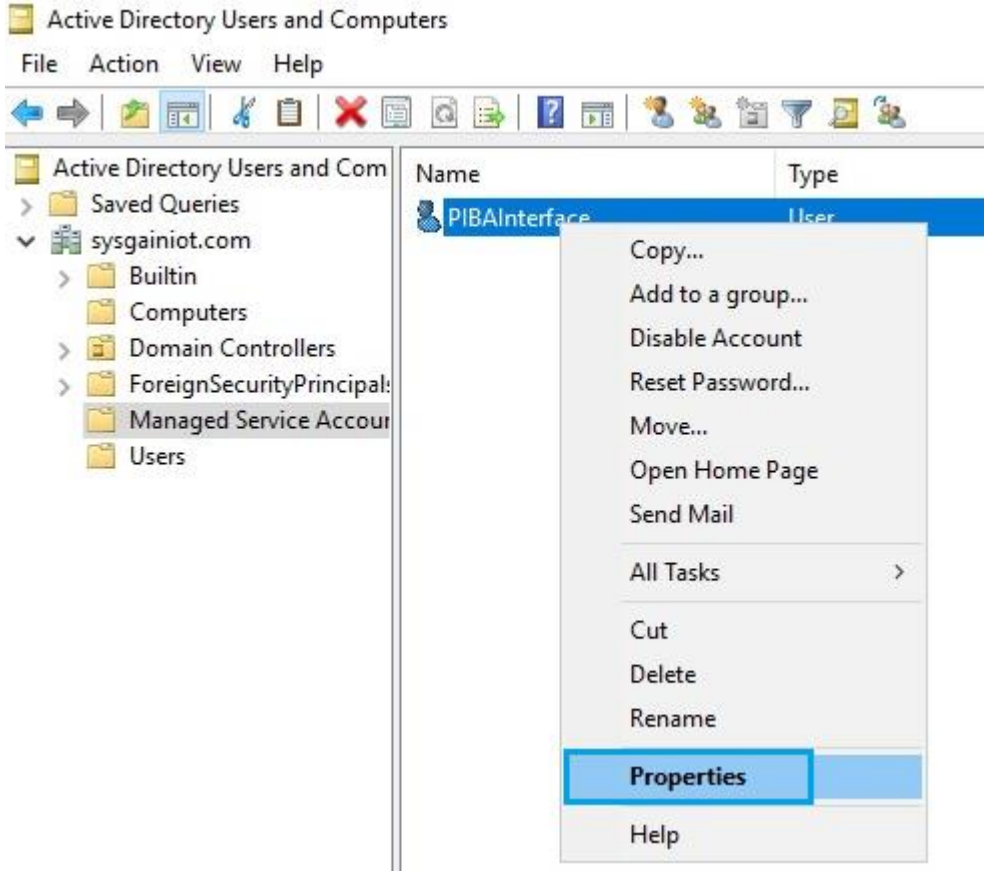
7. Enter the **Password** and uncheck U**ser must change password at next logon**. Click on **Next.**



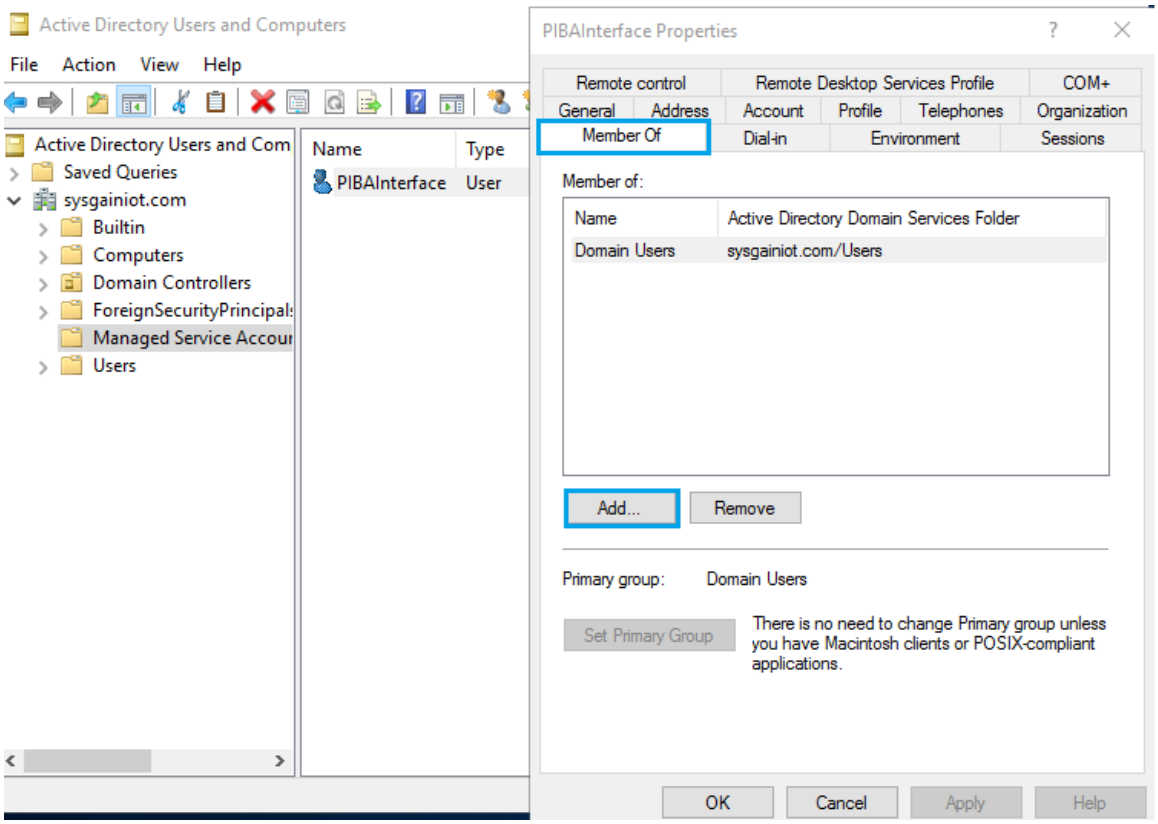
8. Click **Finish** once the object is created.



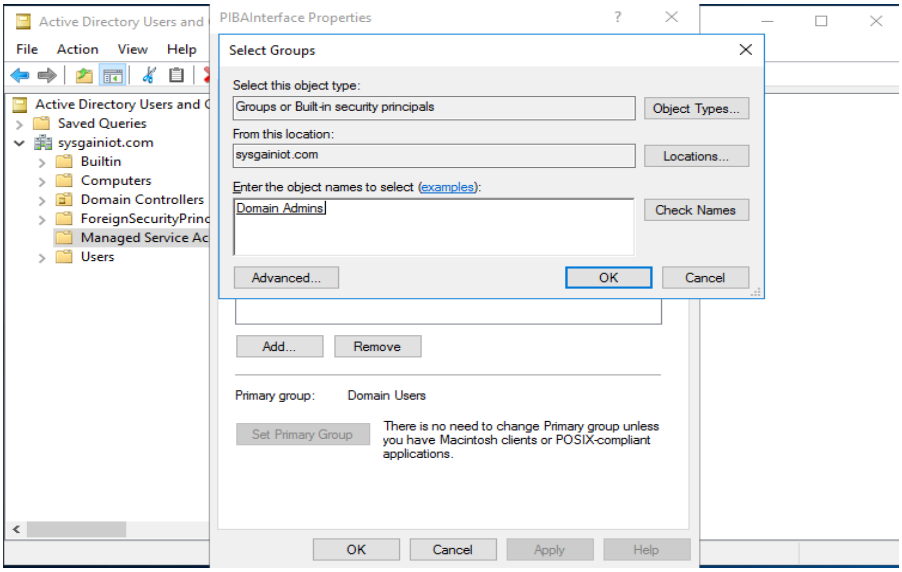
9. Check on the properties of the user created. Right click on the **PIBAInterface** and click on **Properties**.



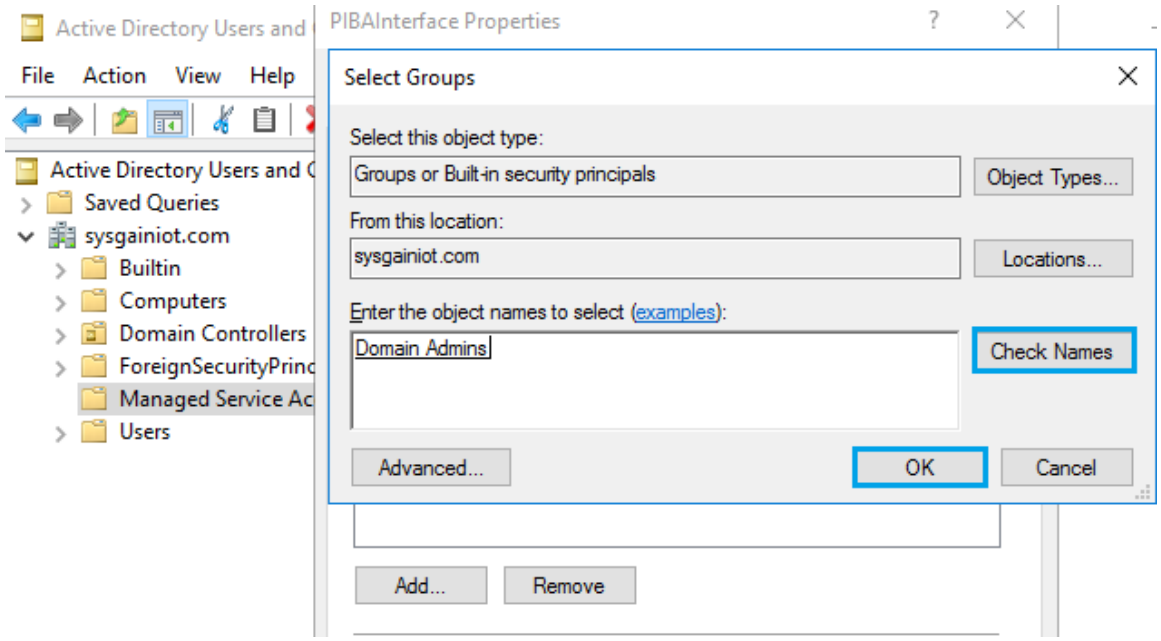
10. A popup will appear. Click on the **Member Of** tab and click the **Add** button.



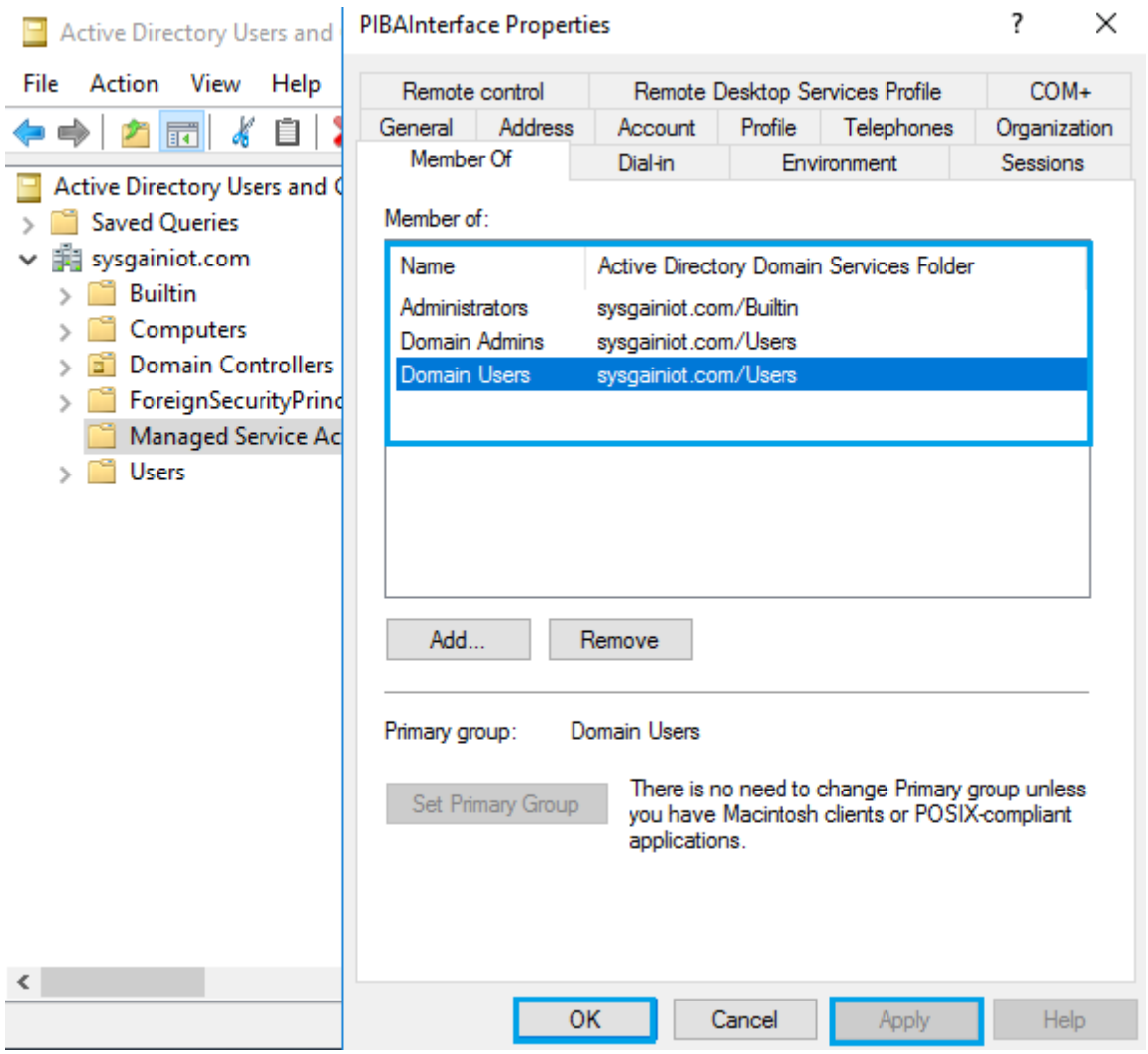
11. Enter the object name as **Domain Admins** and click on **Check Names.** It will display the Domain Admins as object names. Click on **Ok**. After that, click on **Ok** again. You will see the Domain Admin name added to the **Member of** section.



12. Similarly, click on **Add** and enter the object name as **admin** and click on **Check Names**. It will show the **Administrator's** name as an object name, then click on **Ok**. After that click on **Apply** and **Ok**. You should see the Administrators name added to the **Member of** section.

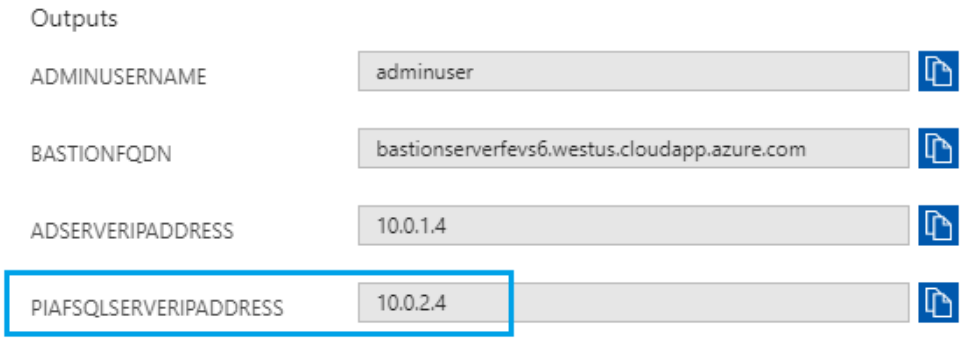


13. You can view the Added names in the **Member of** tab, then click on **Apply** and **OK.**

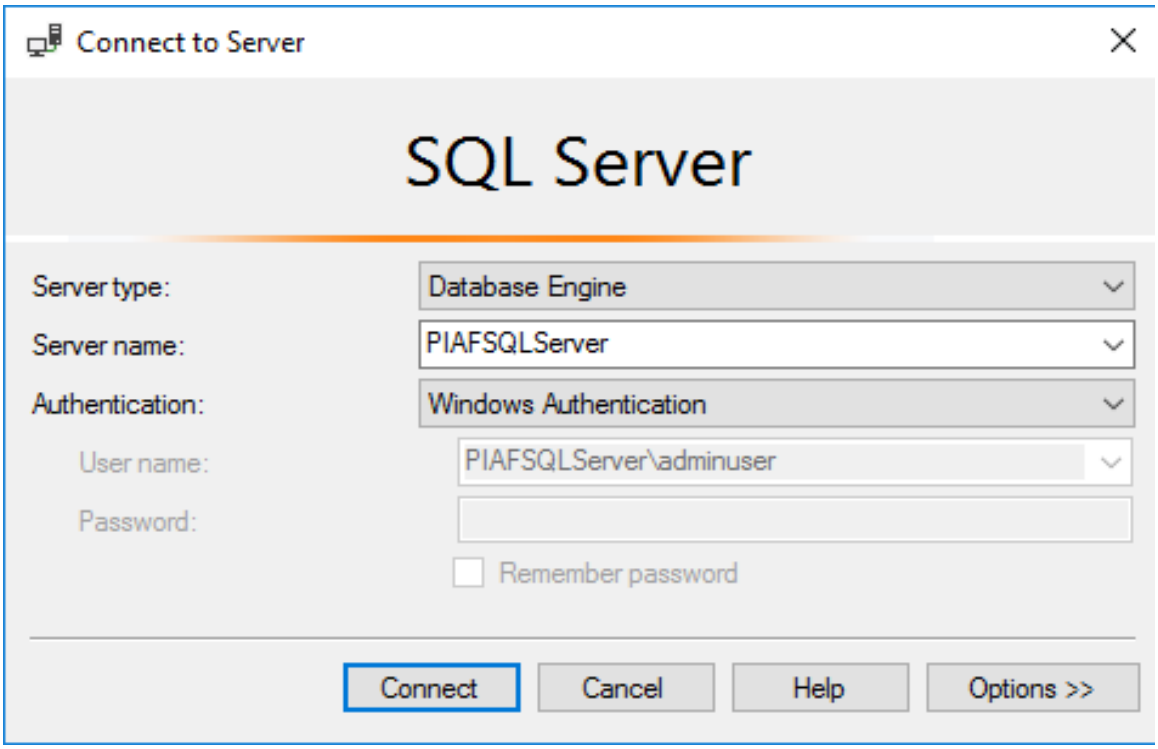


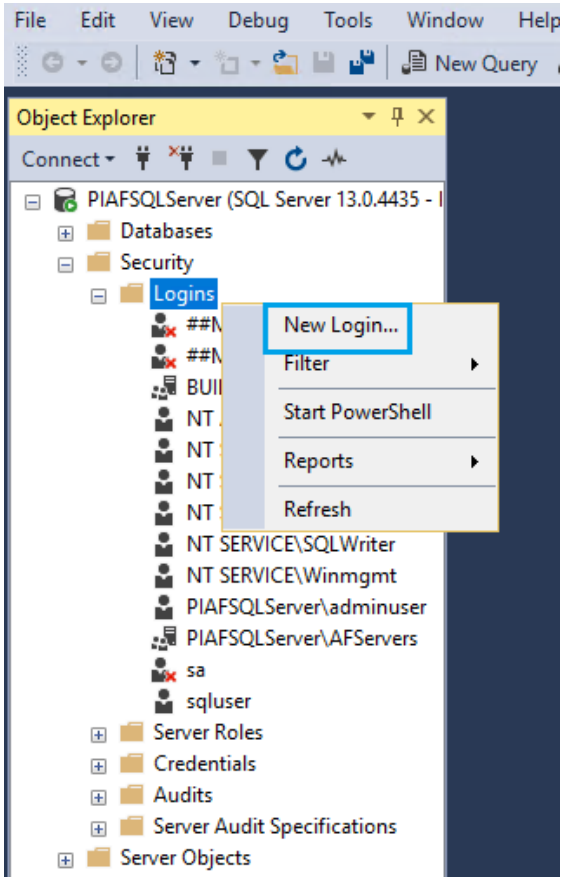
8.1. Create PIBA User in PIAF Server

1. From the Bastion host, connect to the **PIAF** through the private IP address with the credentials provided in the output section.

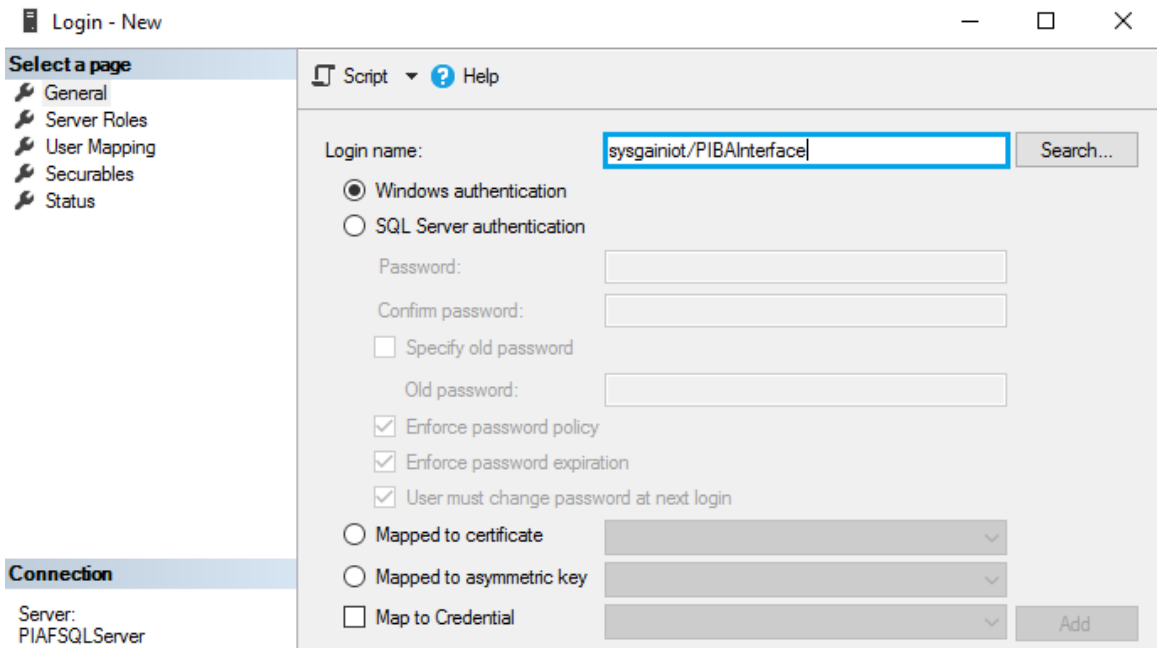


2. After logging in to the PIAF SQL Server, search for **ssms** in start menu to open the open the **SQL Server Management Studio** and create a new login by navigating to **Security** > Right-click on **Logins** and selecting **New Login**.

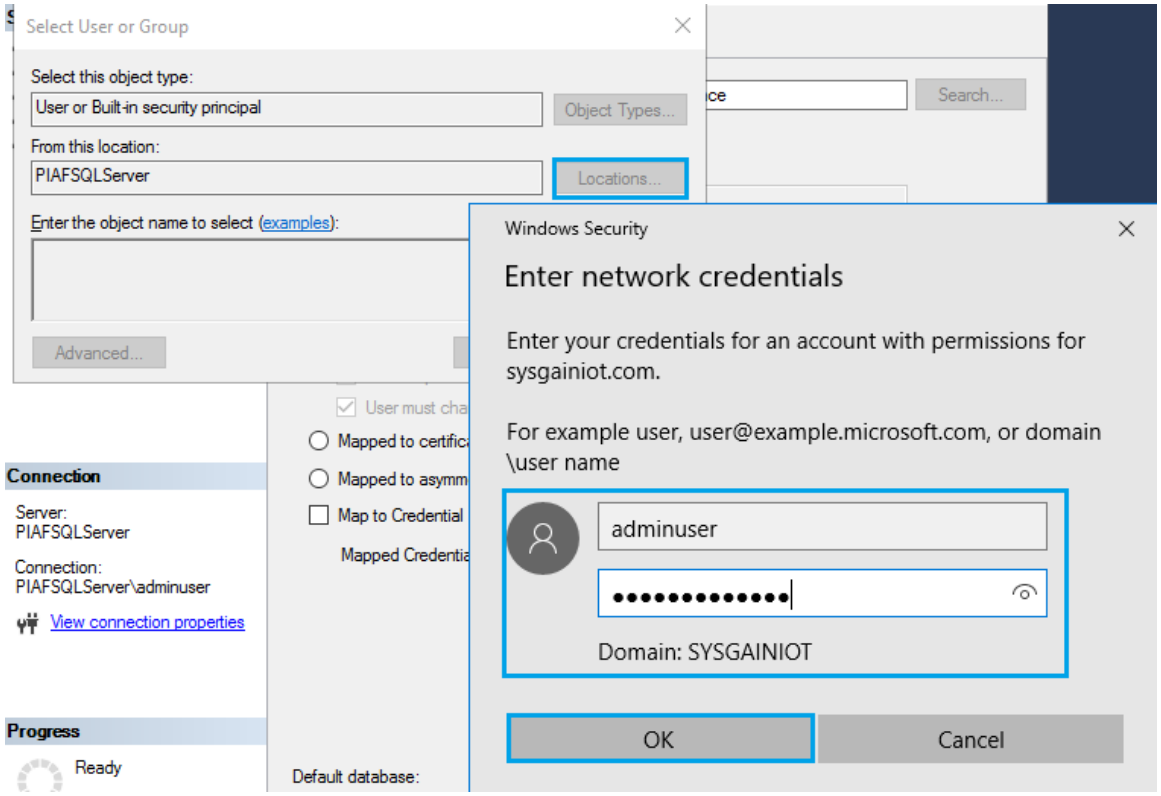

Connect to Server
SQL Server
Server type:
Database Engine
Server name:
PIAFSQLServer
Authentication:
Windows Authentication
User name:
PIAFSQLServer\adminuser
Password:
Remember password
Connect
Cancel
Help
Options >>



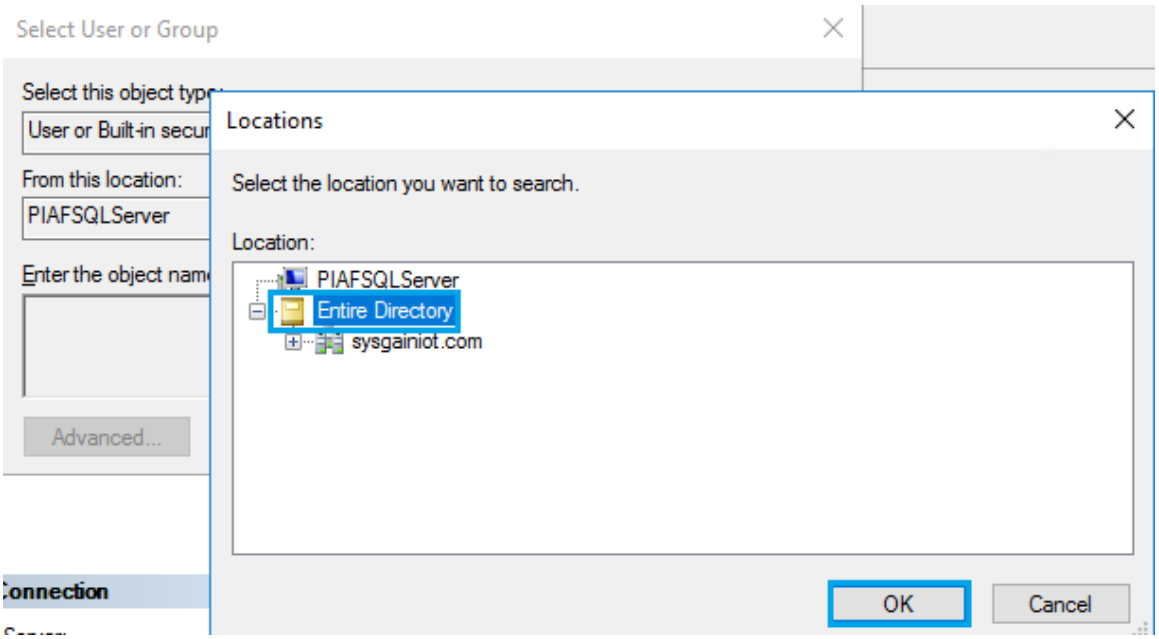
3. Give the login name as **domain name** without .com**/PIBAInterface**, then click on **Search**.



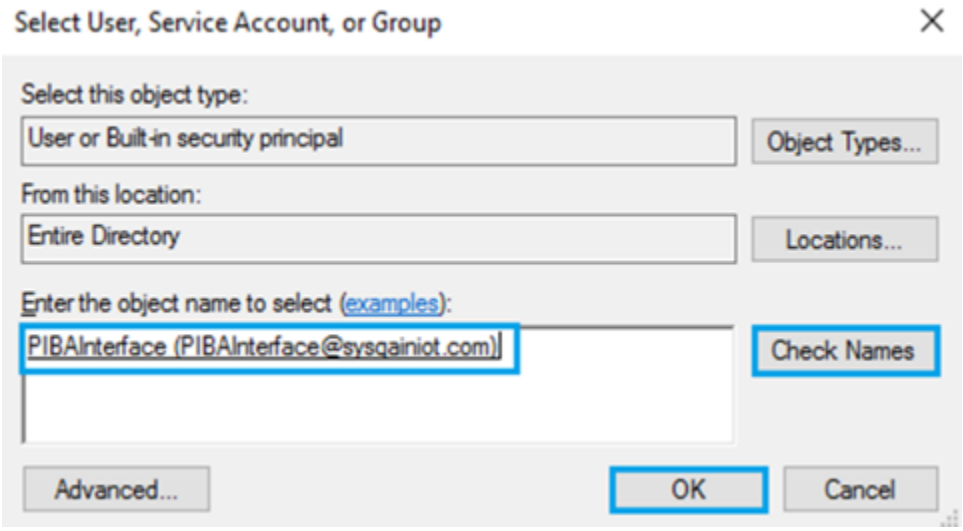
4. Click on **Locations**. You will get a popup box of credentials: enter the SQL server credentials.



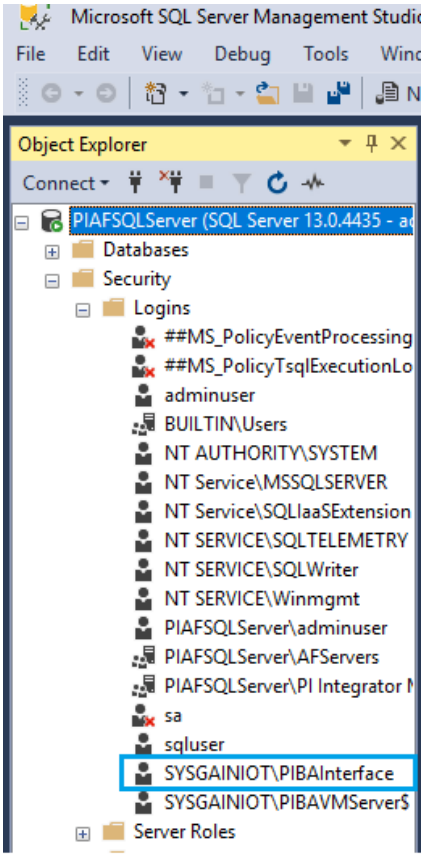
5. Select the **Entire Directory** and click on **OK**.



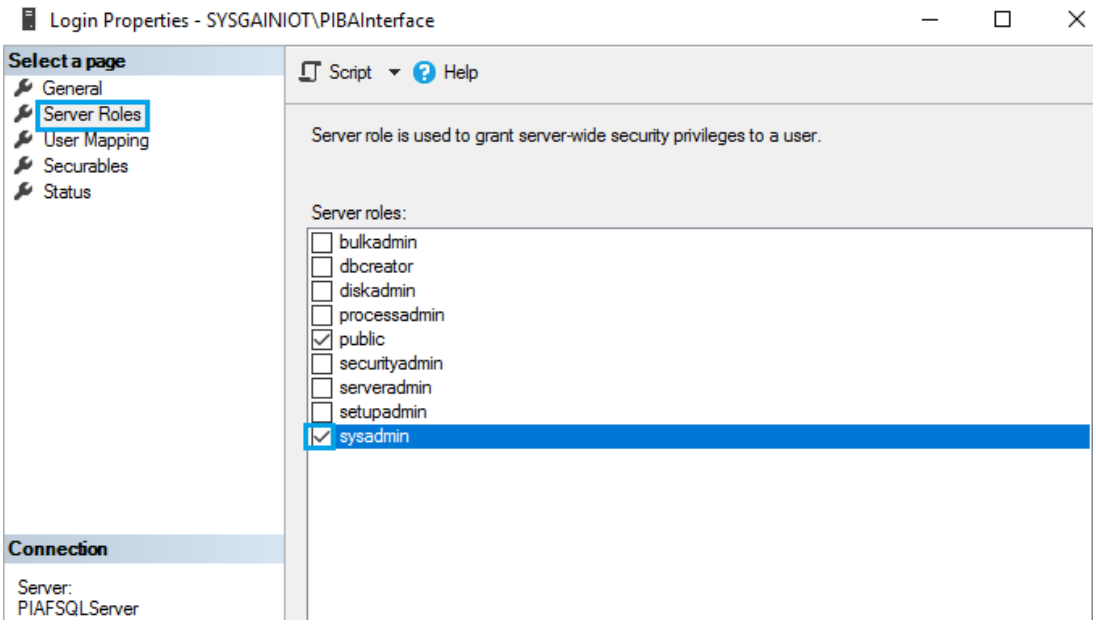
6. Enter the object name as **PIBAInterface** and click on **Check Names**. Then click on **OK**



7. Check for the user you created under the **Logins**.

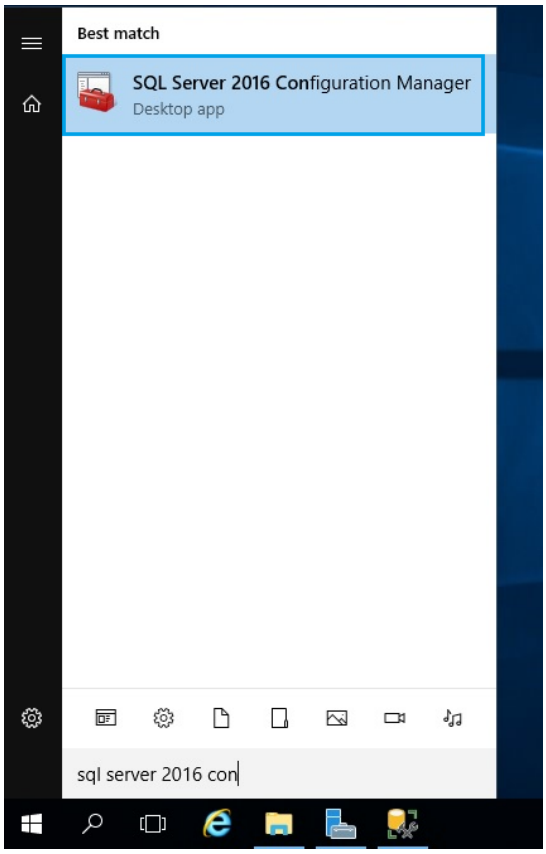


8. Right click on **User (created)** > Right click and select **properties** > click **Server Roles** > check the **sysadmin** box to give permission to the new user.

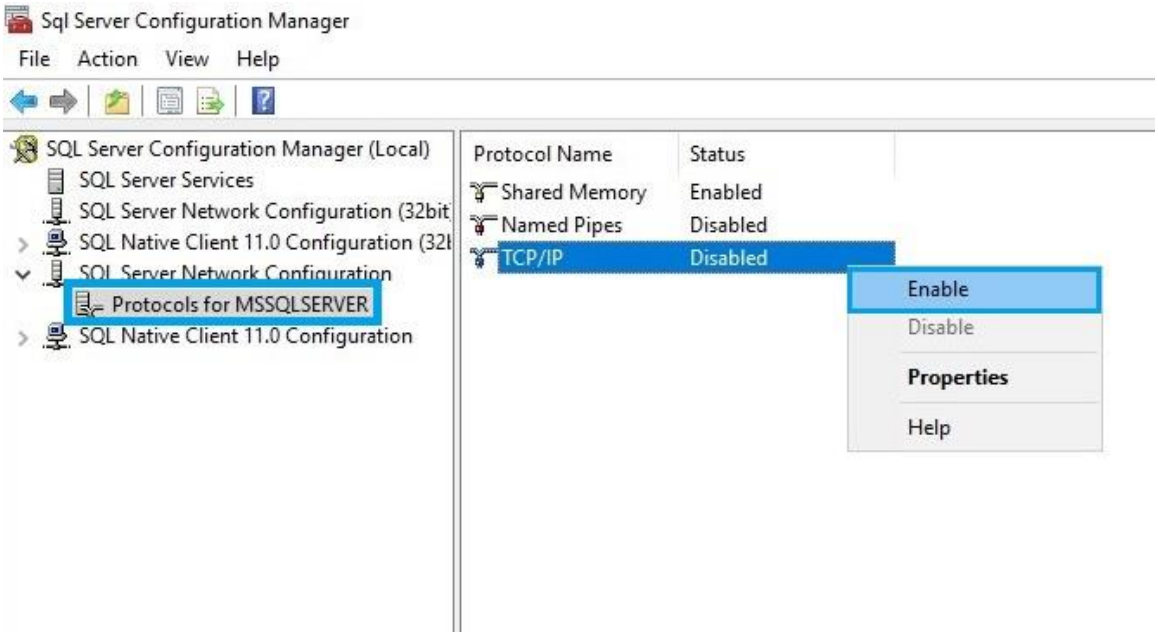


8.2. Enable TCP and Named Pope in SQL Server Configuration Management

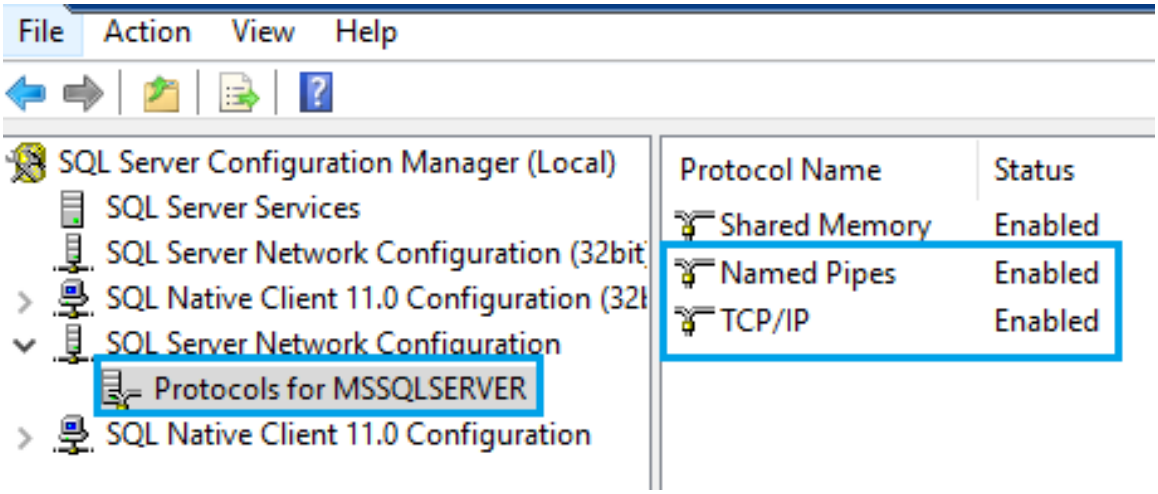
1. From the **Start** menu, navigate to **SQL Server 2016 Configuration Management**.


Best match
SQL Server 2016 Configuration Manager
Desktop app
sql server 2016 con

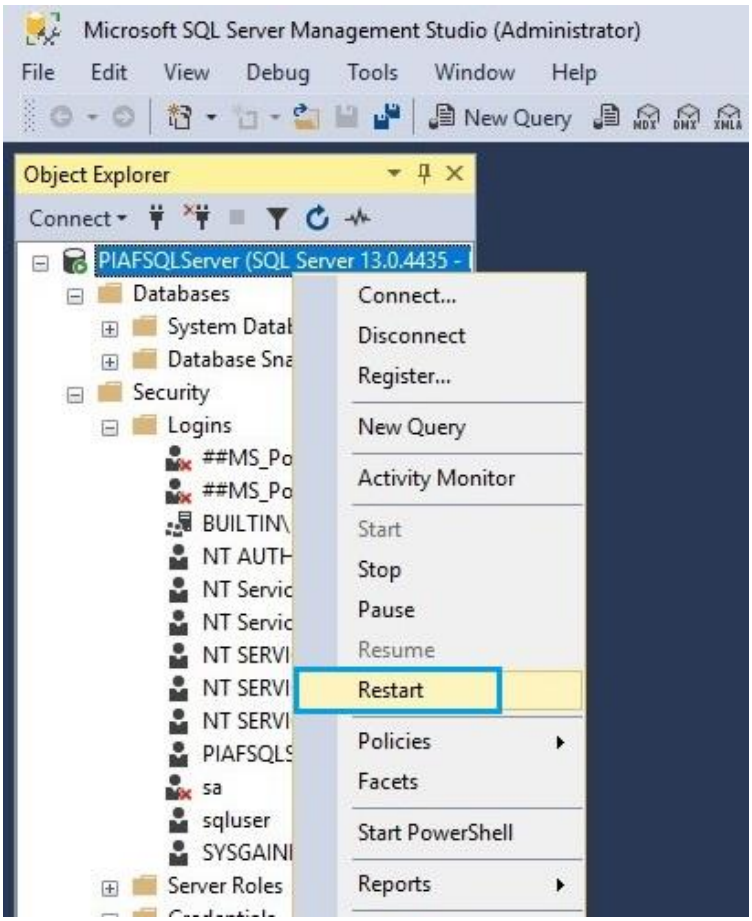
2. Click on **SQL Server Network Configuration** > **Protocols for MSSQLSERVER.**



3. Right click on **TCP/IP**, select **Enable** and click **ok**, then do the same for **Named Pipes.**



4. After making the changes, restart the **PIAFSQLServer,** as shown below. When you click on restart, a dialogue box will ask if you are sure to restart the service. Click **Yes**.



9. Components of PI Server

PI Server is the real-time data storage and distribution engine that powers the PI System. It provides a comprehensive real-time and historical look at operations, enabling users to make timely and impactful decisions.

PI Server is comprised of 3 Components:

- PI Asset Framework
- PI Data Archive
- PI Business Analytics

9.1. PI Asset FrameWork (AF)

PI Asset Framework (AF) is a meta-data structure of data and an integral part of the PI Server. It allows you to build an asset model of the physical objects in your process and

associate asset properties to your data. It is a single repository for asset-centric models, hierarchies, objects, and equipment.

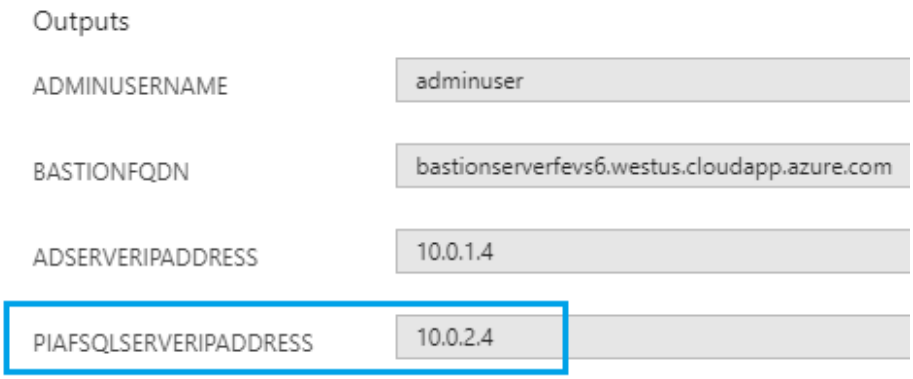
PI Asset Framework can also expose these elements and associated data to non-PI systems via a rich set of data access products. PI AF also includes a number of basic and advanced search capabilities to help users sift through static and real-time information.

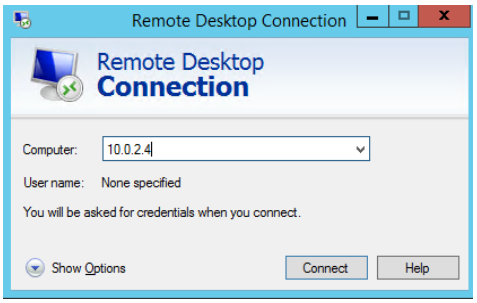
PI Asset Framework also includes features to simplify building, elements including:

- Support for templates
- Object-level security via Identities like the PI Data Archive (new in 2015)
- Support export to or import from XML files
- A sandbox area where an individual can work on changes without impacting other users

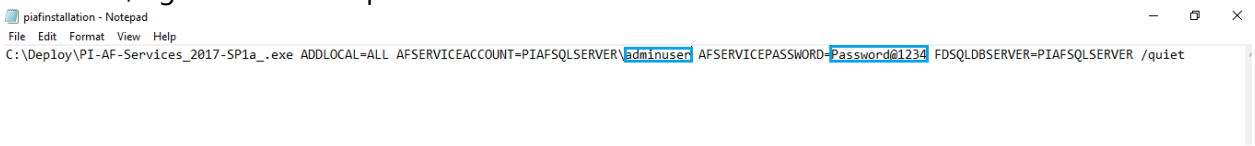
9.1.1. Installation of PIAF Server

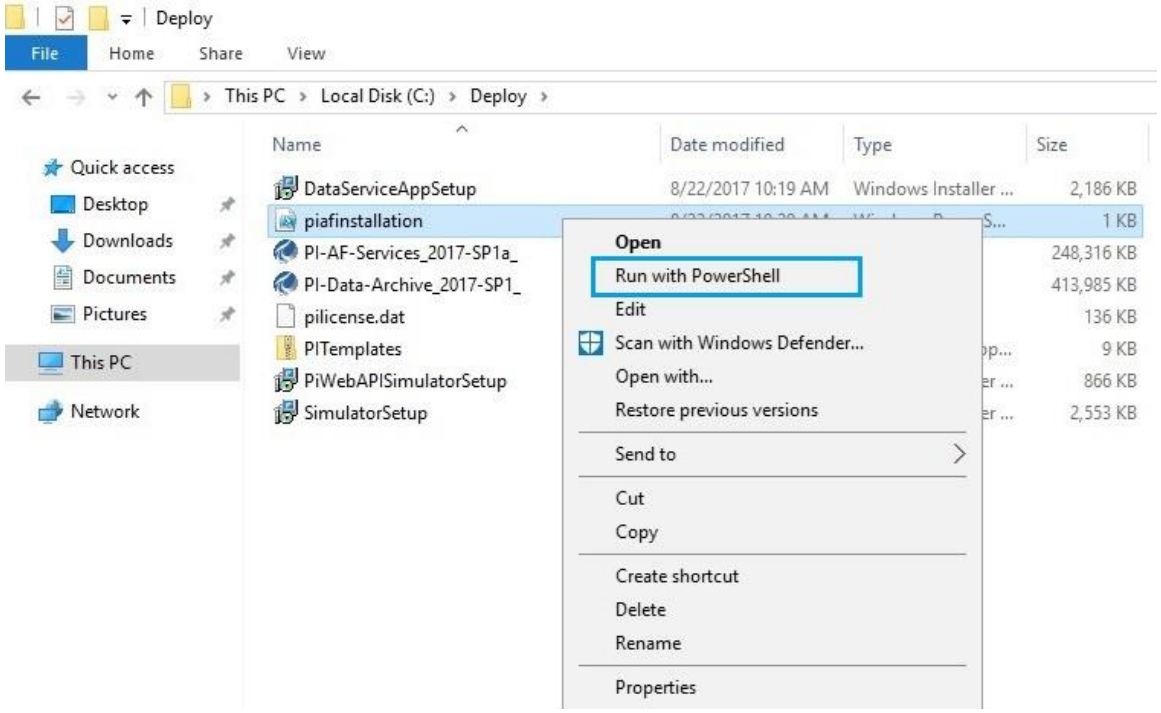
1. Login into **PIAFSQLServer VM** with the Private IP Address from the Bastion Server with the credentials provided in the output section.



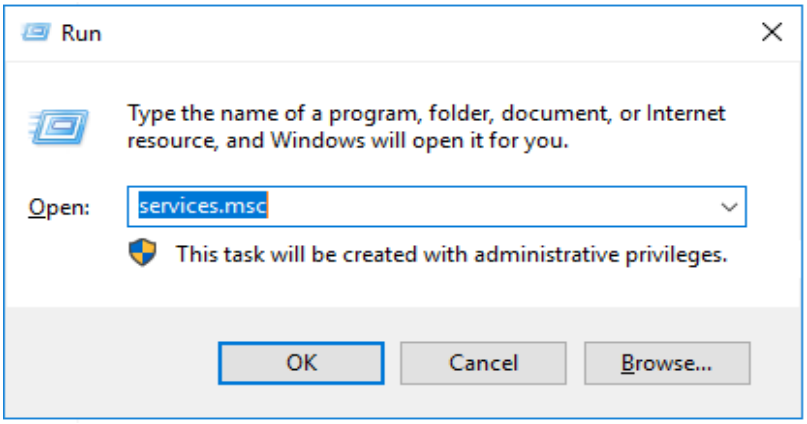


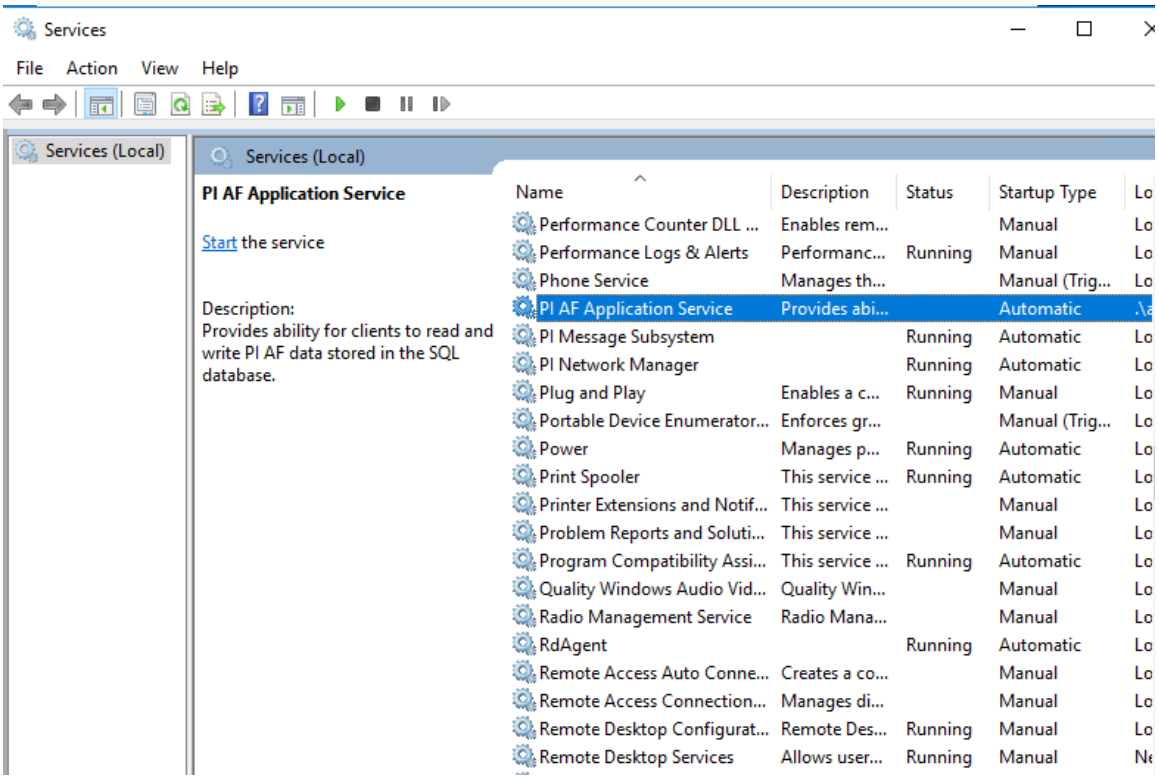
2. Navigate to **Local disk (C:)** > **Deploy** > Right click on **piafinstallation** > Open with Notepad. In the PowerShell script, edit the **adminuser** and **Password@1234** values to update them with your username and password from the PIAFSQLServer and then **save**. After that, right click on the piafinstallation > select **Run with Powershell.**





3. Check if the **piafinstallation** is running using the **services.msc** command in the Run tool (do a Windows search for "Run").





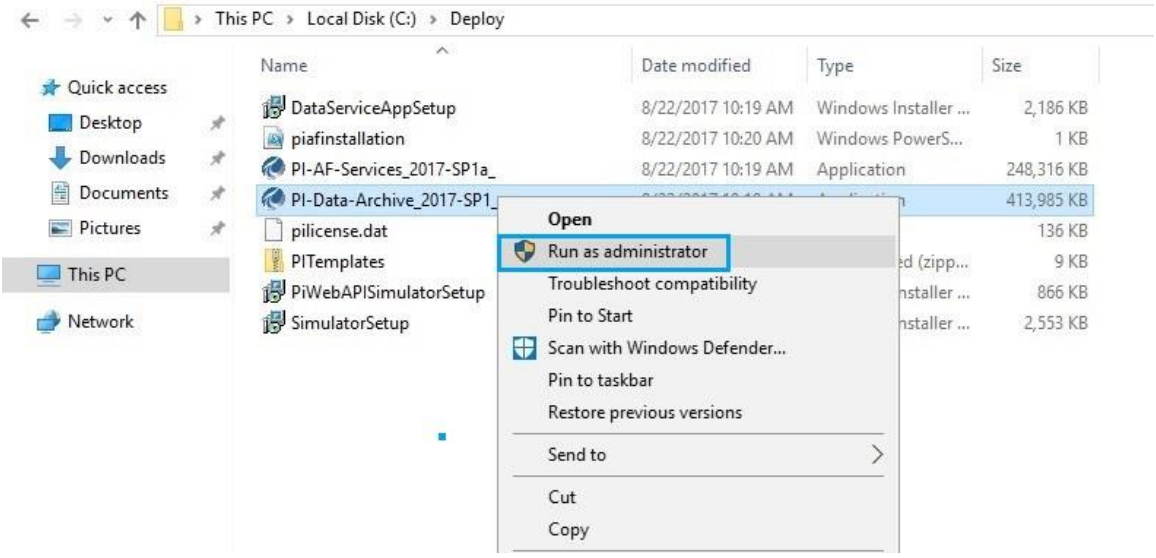
9.2. PI Data Archive (PIDA)

The PI Data Archive is a component of the PI Server that provides efficient storage and archiving of time series data, enabling high performance data retrieval by client software. Traditionally, the PI Data Archive was referred to as the "PI Server", but because the PI server itself has incorporated so many new capabilities, including data modeling and analytics, its name has been changed.

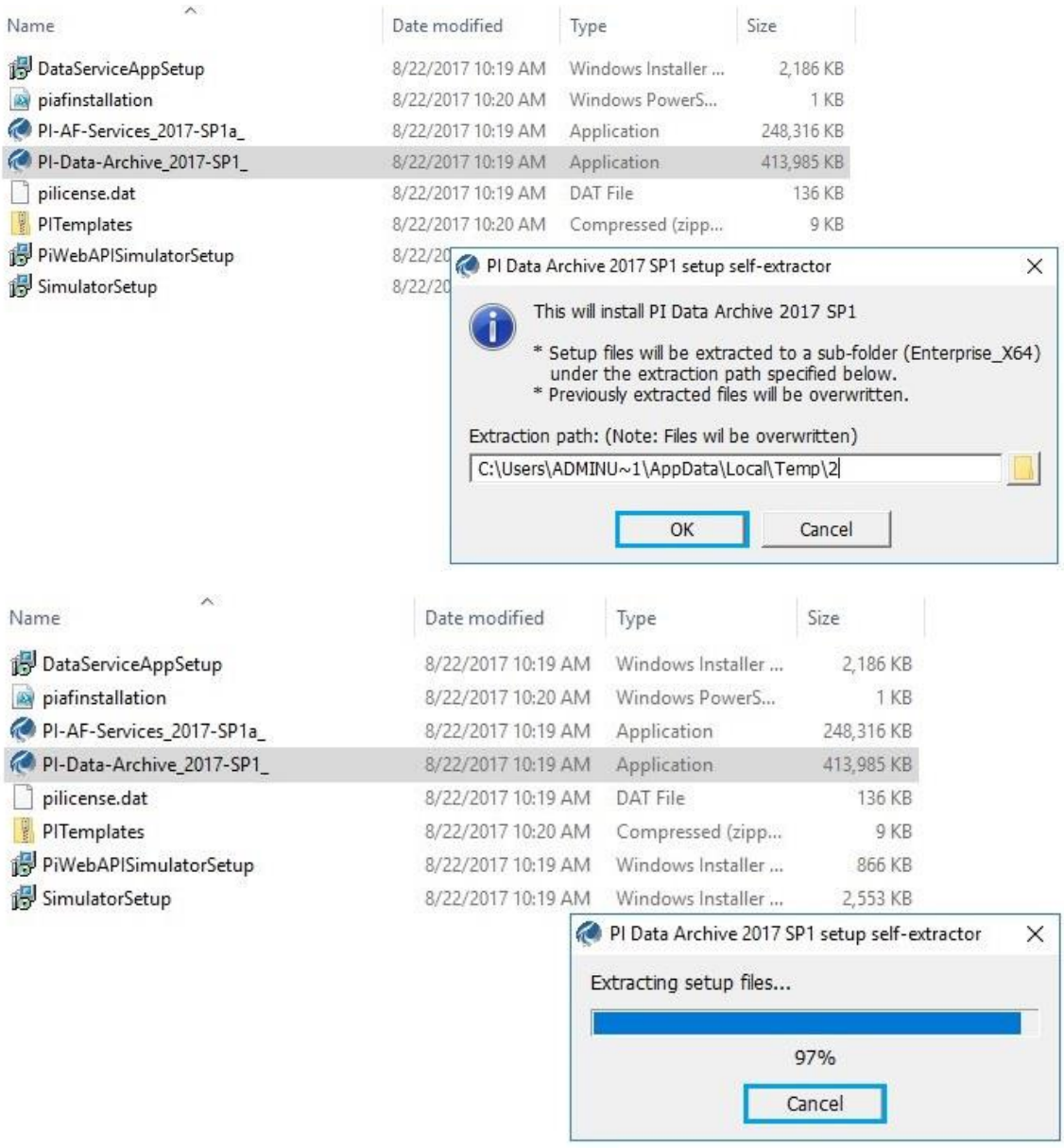
The PI Data Archive collects, stores, and organizes data from data sources, providing an information infrastructure. The PI Server also includes tools for analytics, alerts, and auditing. The PI Server may be connected to almost any existing automation, lab, or information system. Operators, engineers, managers, and other plant personnel can use client applications to connect to the PI Server to view data stored in the PI Server or in external data archive systems.

9.2.1. Installation of Data Archive (PIDA)

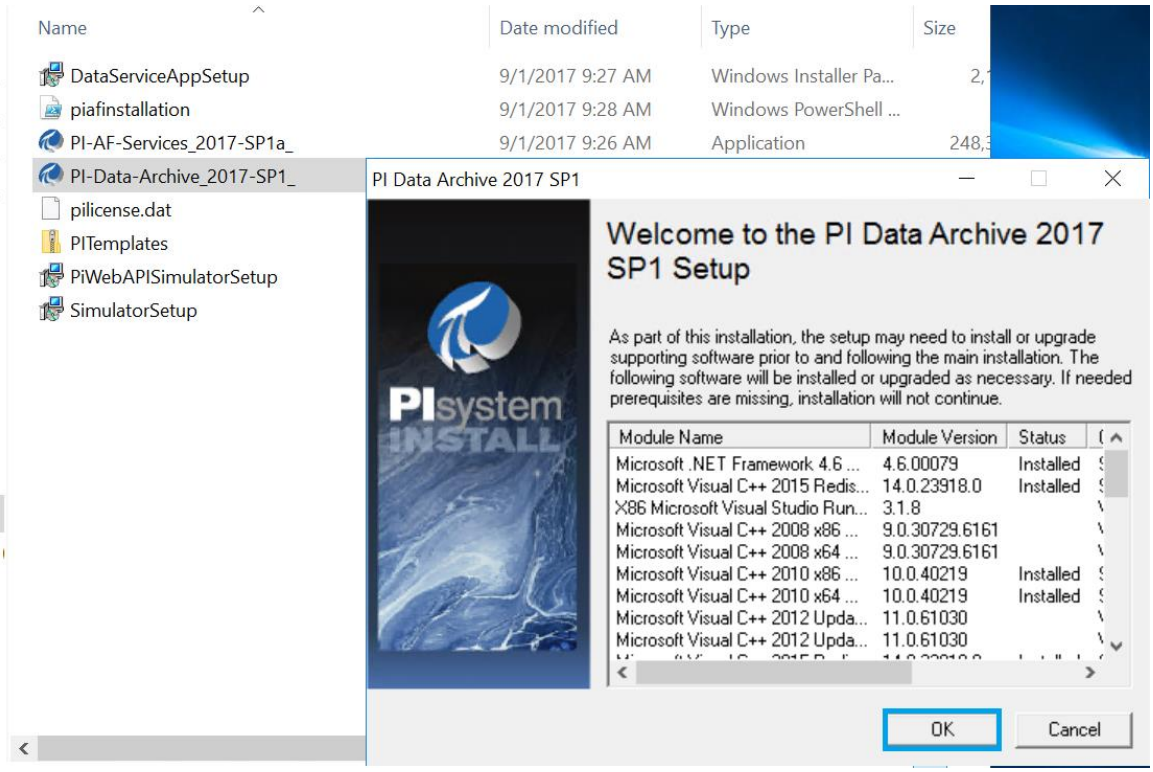
1. Navigate to **Local disk (C:)** > **Deploy** > select **PI-Data-archive_2017-SP1** > right click and **Run as administrator**.



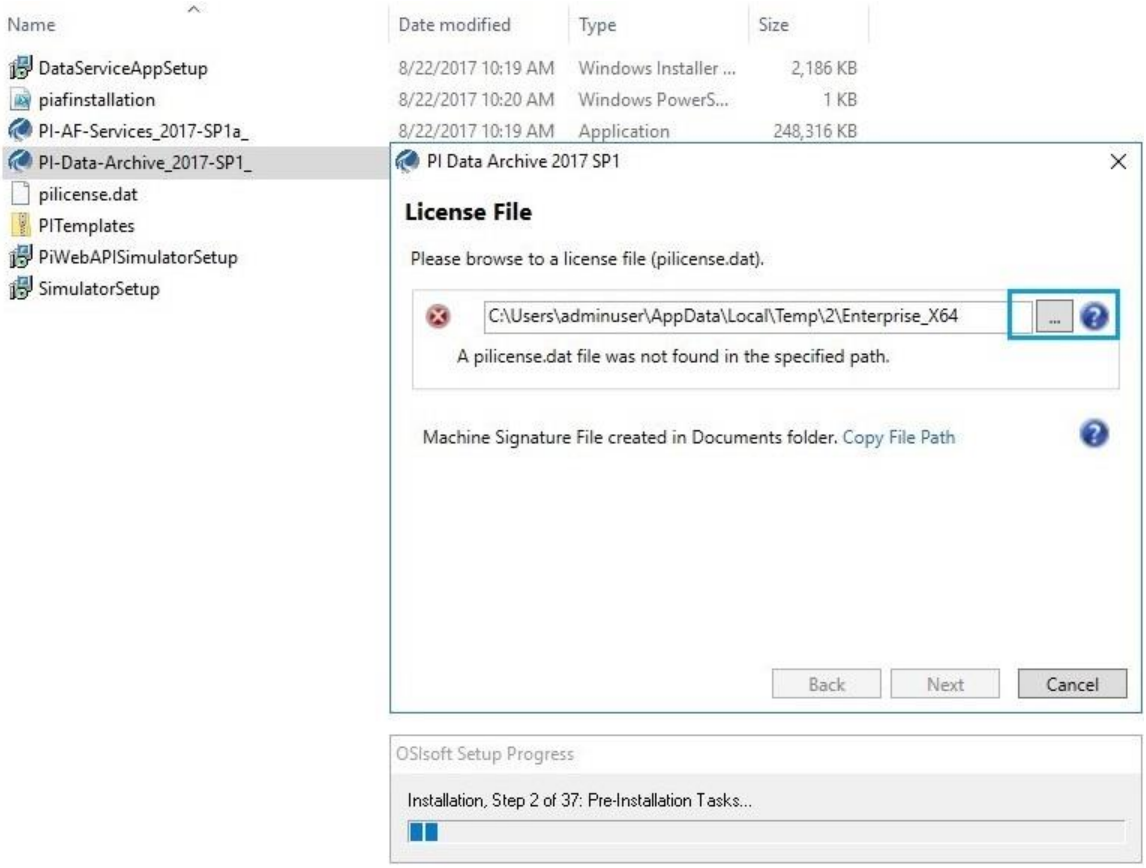
2. Click on **OK**.


Name
Date modified
Type
Size
DataServiceAppSetup 8/22/2017 10:19 AM Windows Installer ... 2,186 KB
piafinstallation 8/22/2017 10:20 AM Windows PowerS... 1 KB
PI-AF-Services_2017-SP1a_ 8/22/2017 10:19 AM Application 248,316 KB
PI-Data-Archive_2017-SP1_ 8/22/2017 10:19 AM Application 413,985 KB
pilicense.dat 8/22/2017 10:19 AM DAT File 136 KB
PITemplates 8/22/2017 10:20 AM Compressed (zipp... 9 KB
PiWebAPISimulatorSetup
SimulatorSetup
PI Data Archive 2017 SP1 setup self-extractor
This will install PI Data Archive 2017 SP1
* Setup files will be extracted to a sub-folder (Enterprise_X64) under the extraction path specified below.
* Previously extracted files will be overwritten.
Extraction path: (Note: Files wil be overwritten)
C:\Users\ADMINU~1\AppData\Local\Temp\2
OK
Cancel
Name
Date modified
Type
Size
DataServiceAppSetup 8/22/2017 10:19 AM Windows Installer ... 2,186 KB
piafinstallation 8/22/2017 10:20 AM Windows PowerS... 1 KB
PI-AF-Services_2017-SP1a_ 8/22/2017 10:19 AM Application 248,316 KB
PI-Data-Archive_2017-SP1_ 8/22/2017 10:19 AM Application 413,985 KB
pilicense.dat 8/22/2017 10:19 AM DAT File 136 KB
PITemplates 8/22/2017 10:20 AM Compressed (zipp... 9 KB
PiWebAPISimulatorSetup 8/22/2017 10:19 AM Windows Installer ... 866 KB
SimulatorSetup 8/22/2017 10:19 AM Windows Installer ... 2,553 KB
PI Data Archive 2017 SP1 setup self-extractor
Extracting setup files...
97%
Cancel

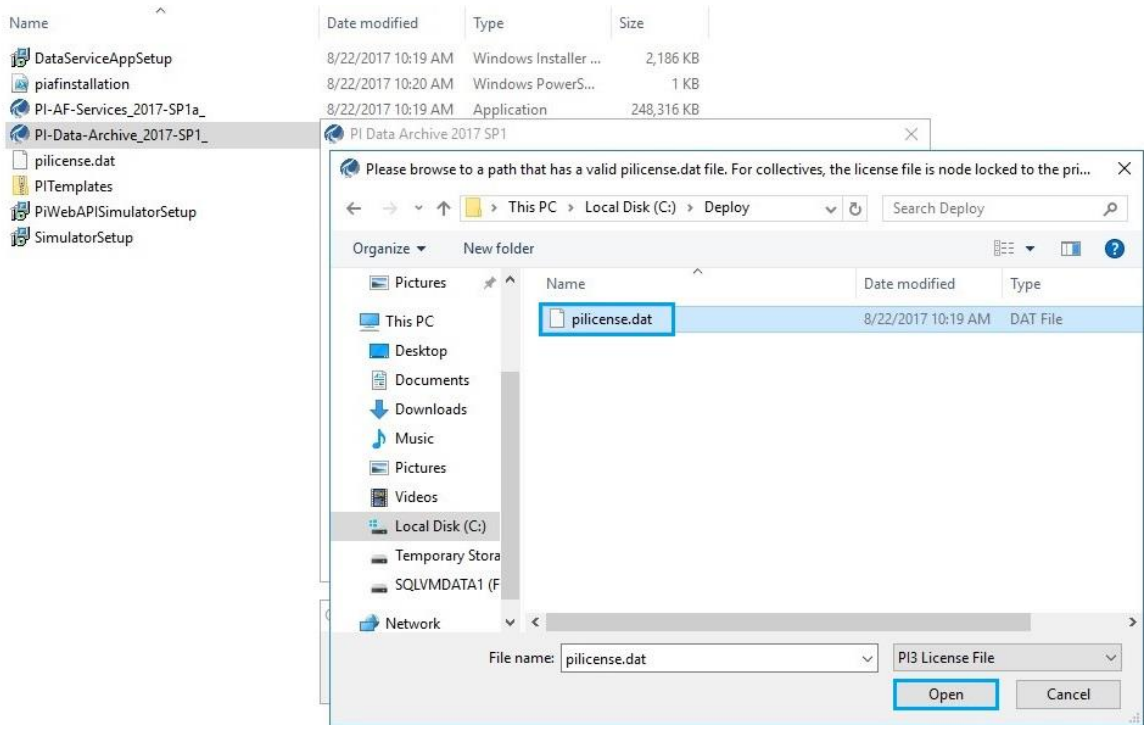
3. Click on **OK**.


Name
Date modified
Type
Size
DataServiceAppSetup
9/1/2017 9:27 AM
Windows Installer Pa...
piafinstallation
9/1/2017 9:28 AM
Windows PowerShell ...
PI-AF-Services_2017-SP1a_
9/1/2017 9:26 AM
Application
PI-Data-Archive_2017-SP1_
pilicense.dat
PITemplates
PiWebAPISimulatorSetup
SimulatorSetup
PI Data Archive 2017 SP1
PIsystem
INSTALL
Welcome to the PI Data Archive 2017 SP1 Setup
As part of this installation, the setup may need to install or upgrade supporting software prior to and following the main installation. The following software will be installed or upgraded as necessary. If needed prerequisites are missing, installation will not continue.
Module Name
Module Version
Status
Microsoft .NET Framework 4.6 ...
4.6.00079
Installed
Microsoft Visual C++ 2015 Redis...
14.0.23918.0
Installed
X86 Microsoft Visual Studio Run...
3.1.8
Microsoft Visual C++ 2008 x86 ...
9.0.30729.6161
Microsoft Visual C++ 2008 x64 ...
9.0.30729.6161
Microsoft Visual C++ 2010 x86 ...
10.0.40219
Installed
Microsoft Visual C++ 2010 x64 ...
10.0.40219
Installed
Microsoft Visual C++ 2012 Upda...
11.0.61030
Microsoft Visual C++ 2012 Upda...
11.0.61030
OK
Cancel

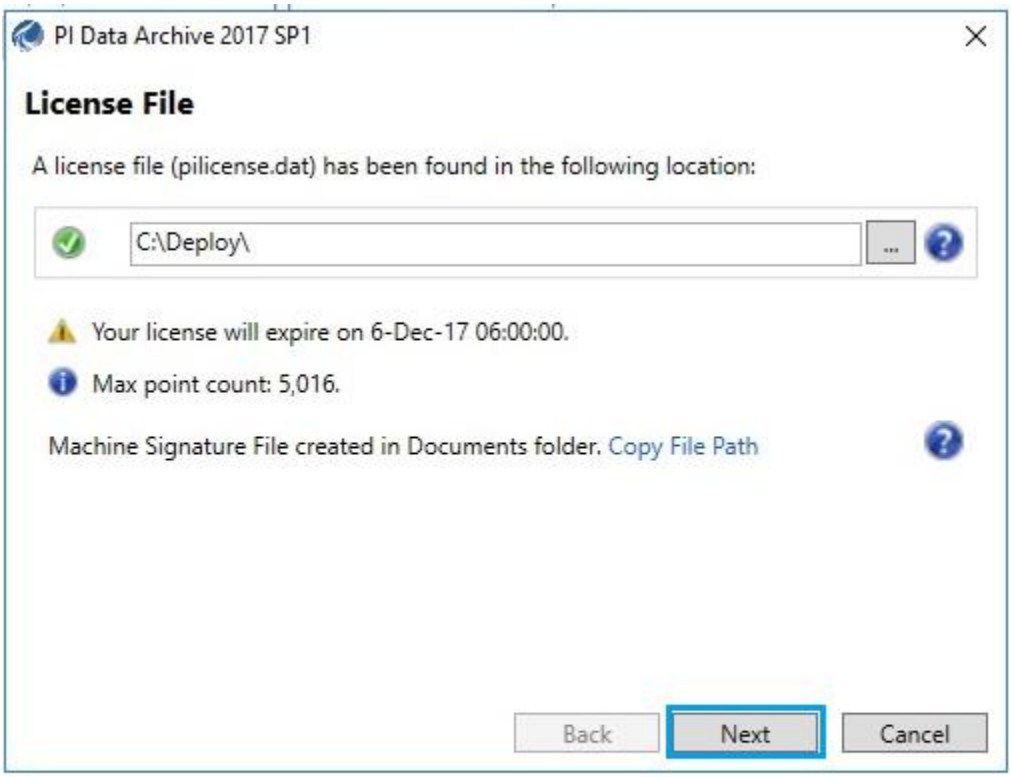
4. After completion of extracting setup files, click on **OK**.

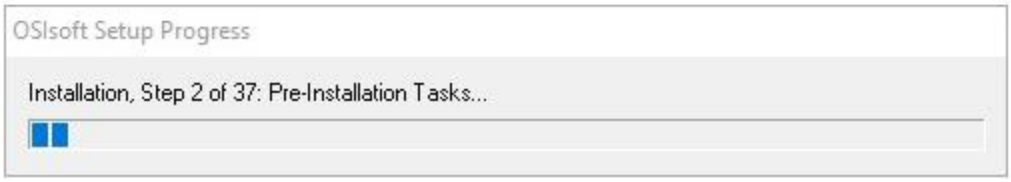


5. Click on the browse option, then navigate to the **Local disk (C:)** > **Deploy** > select **pilicense.dat** and click on **Open.**

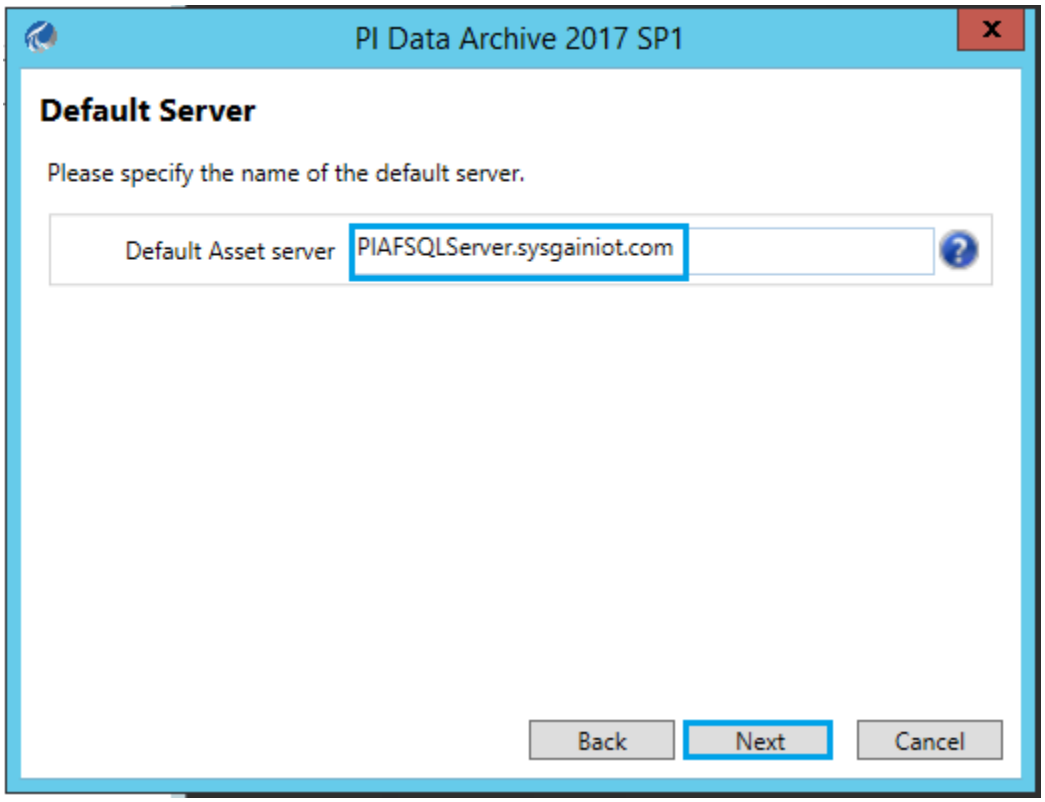


6. After that, click on **Next**.

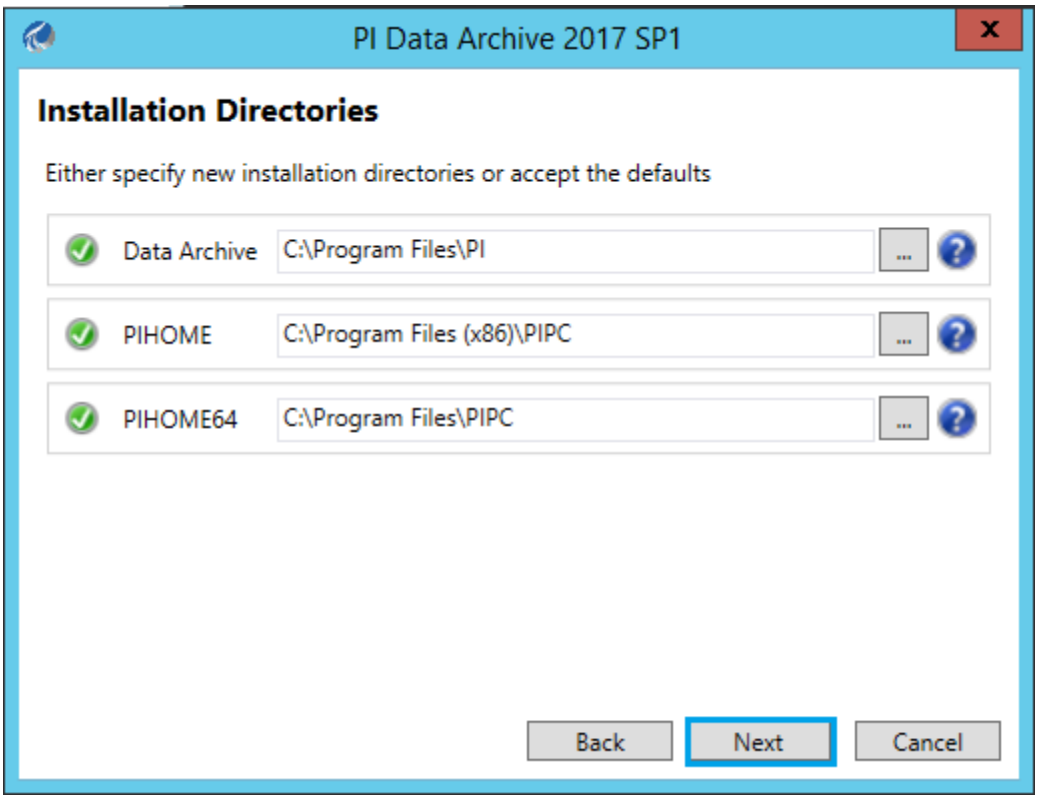


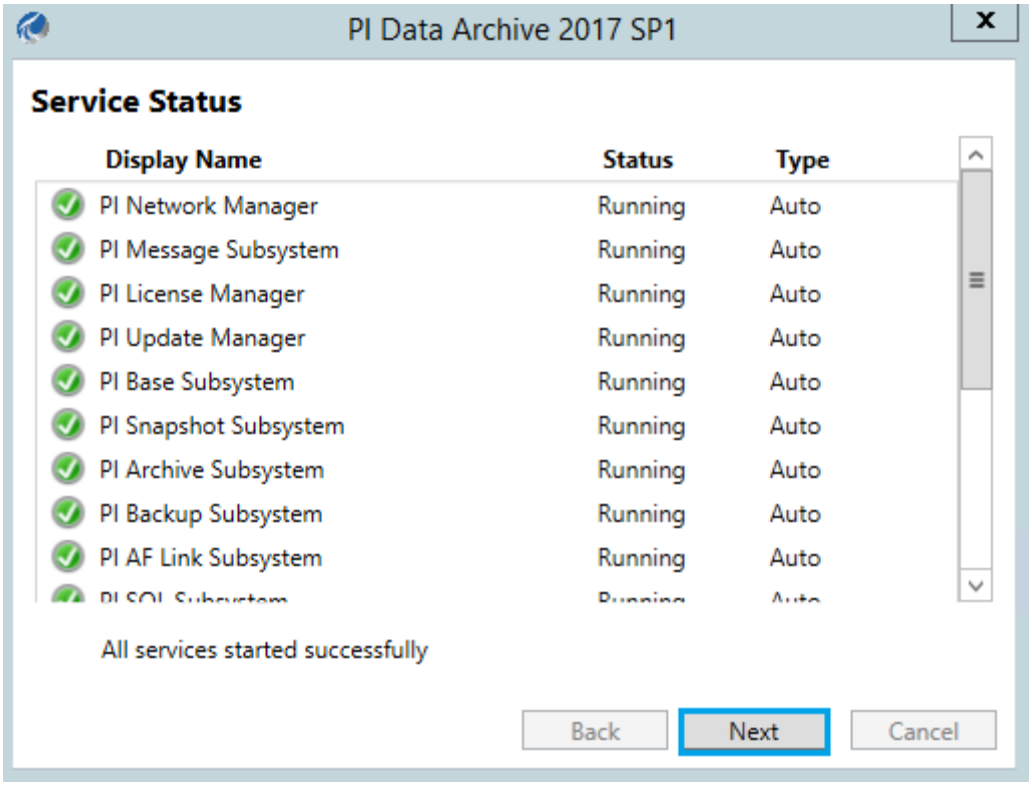


7. Add the domain name to the **Default Asset server** and click on **Next**.

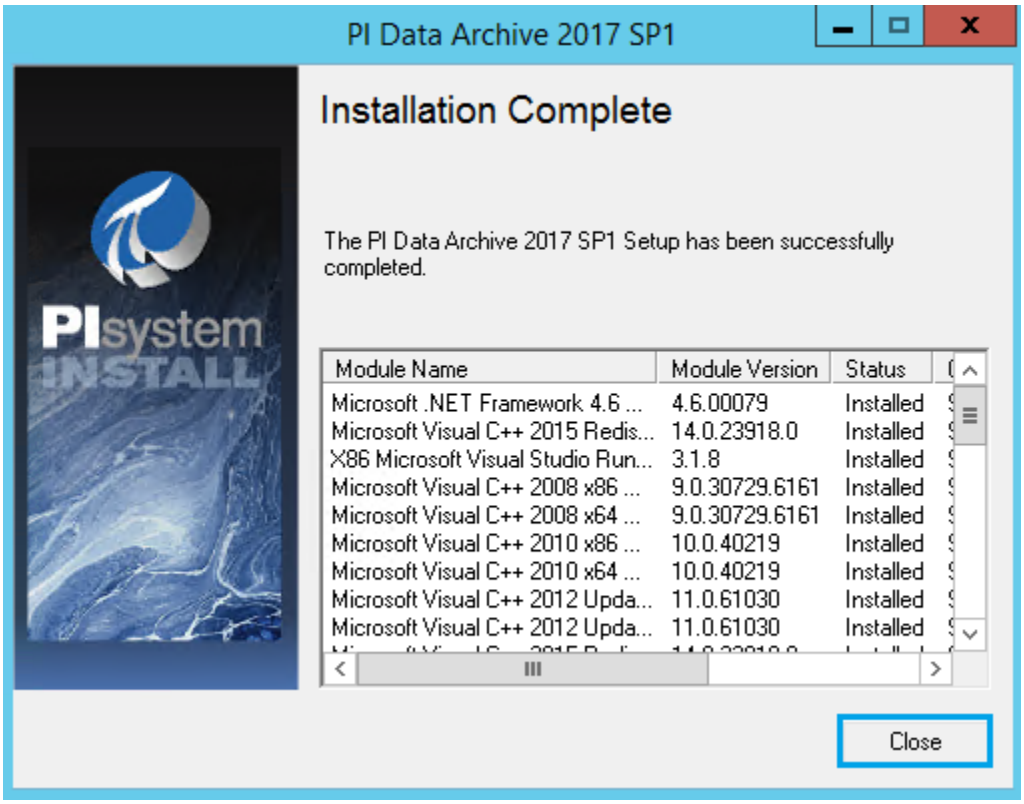


8. Click on **Next**. After getting installation directories, click **Next** again.



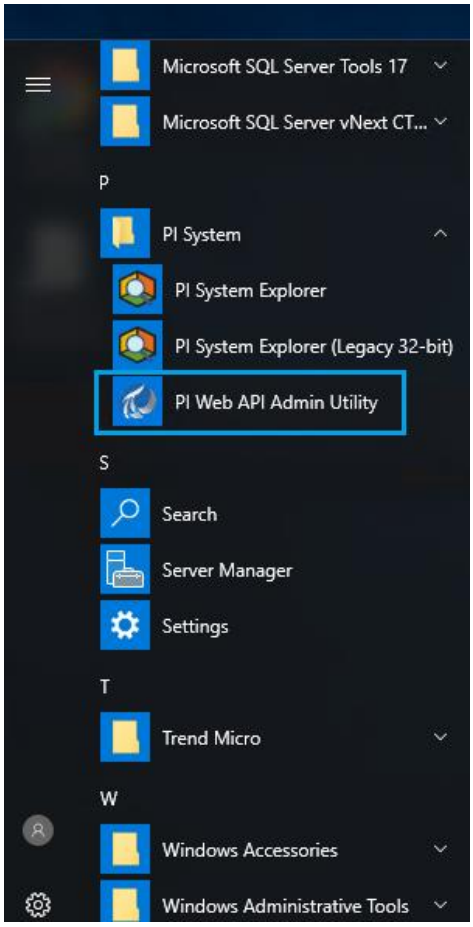


9. Click on **Close** once the installation is completed.

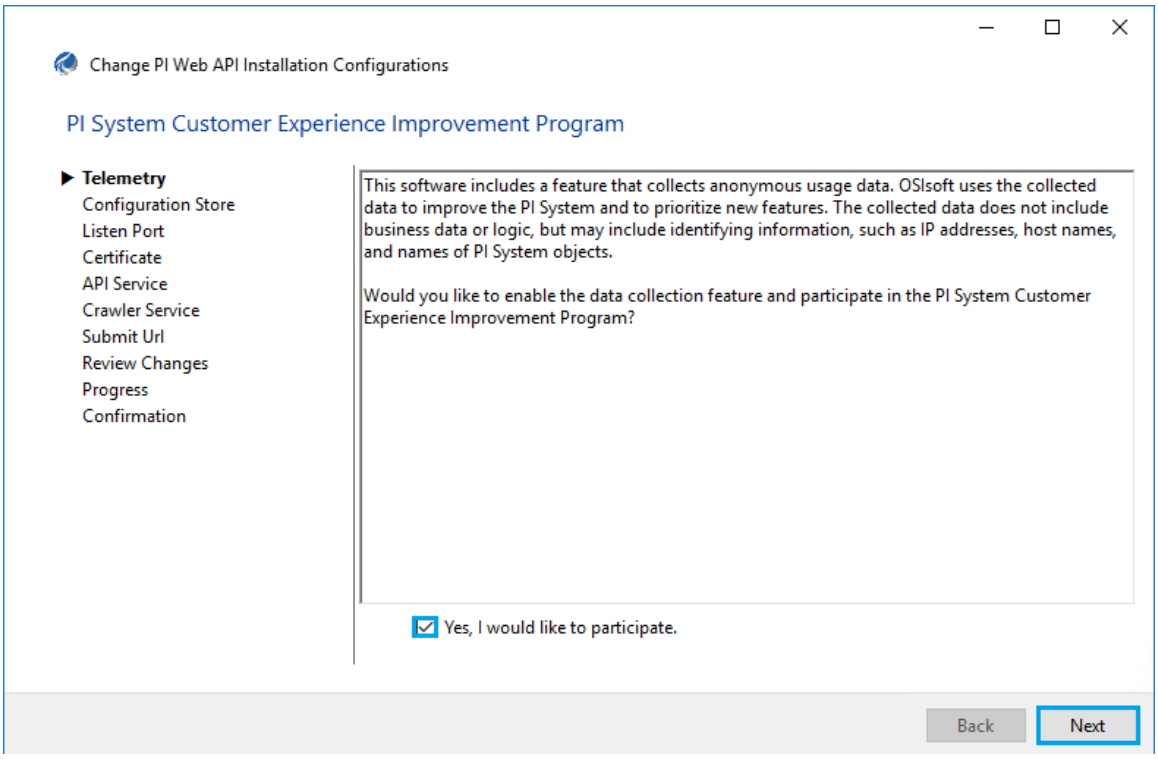


9.3. PI Web API Utility

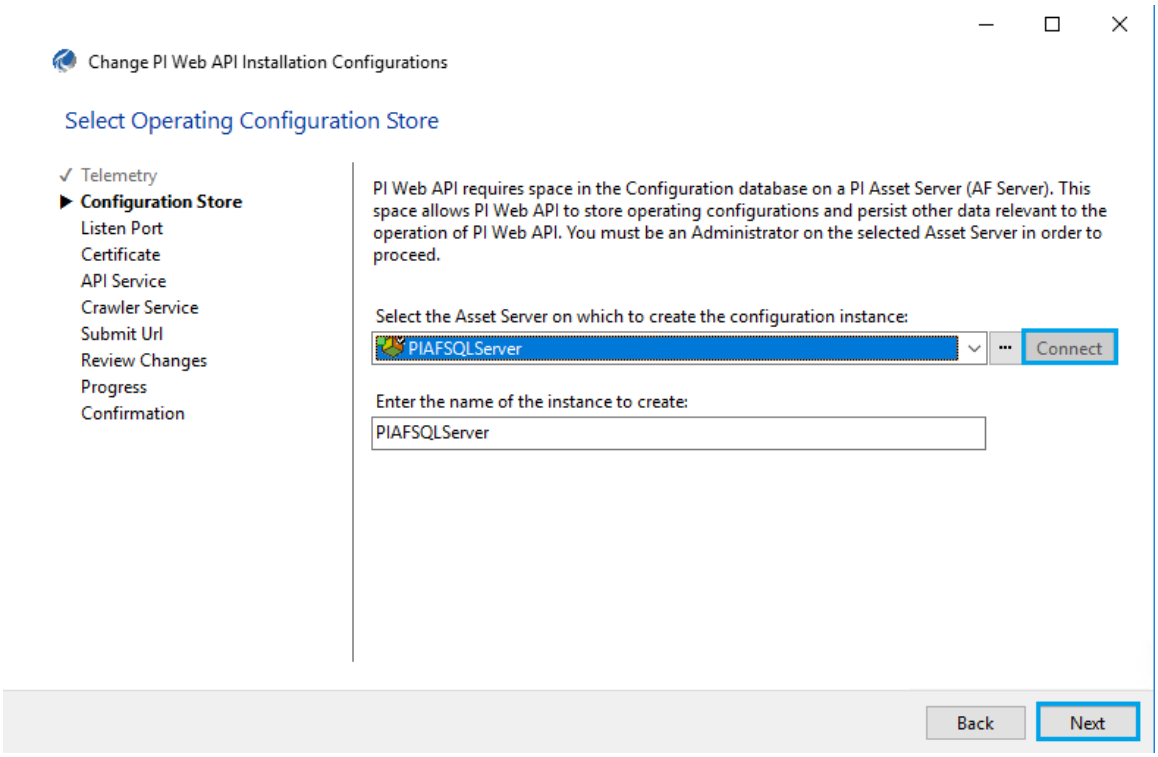
1. Navigate to **PI System > PI Web API Admin Utility** from the Start menu.



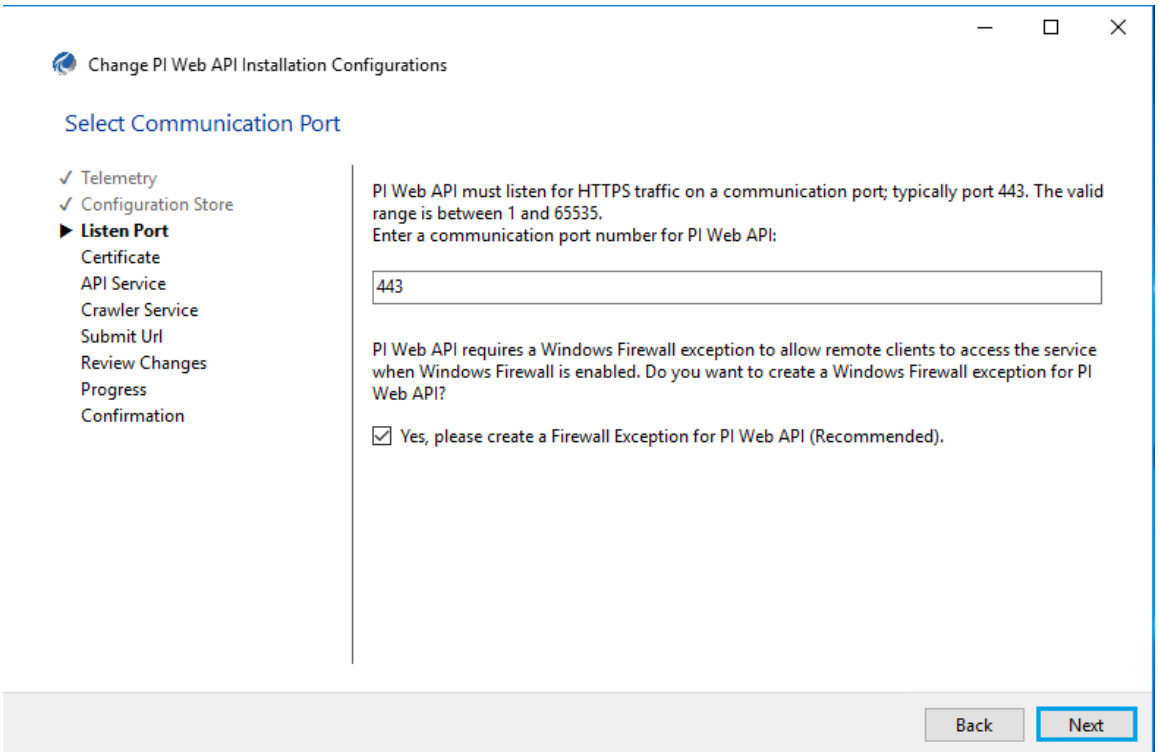
2. Check the **Yes, I would like to participate** dialog box and click on **Next**.



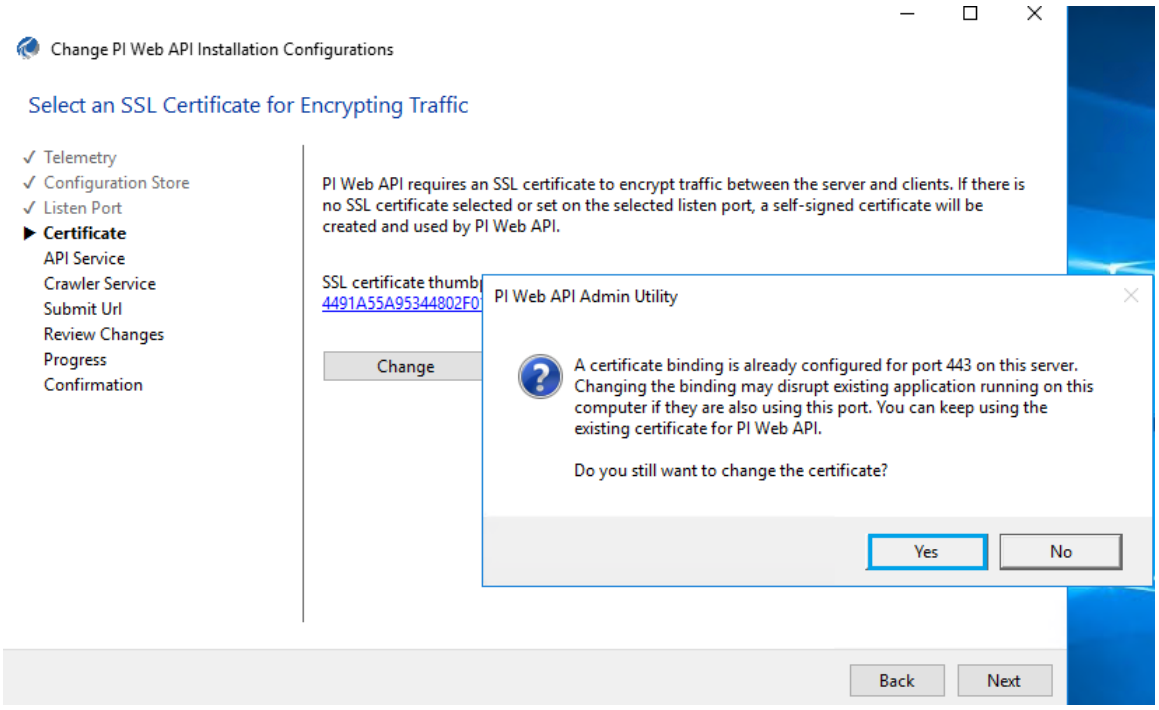
3. Select **Connect** and click on **Next**.



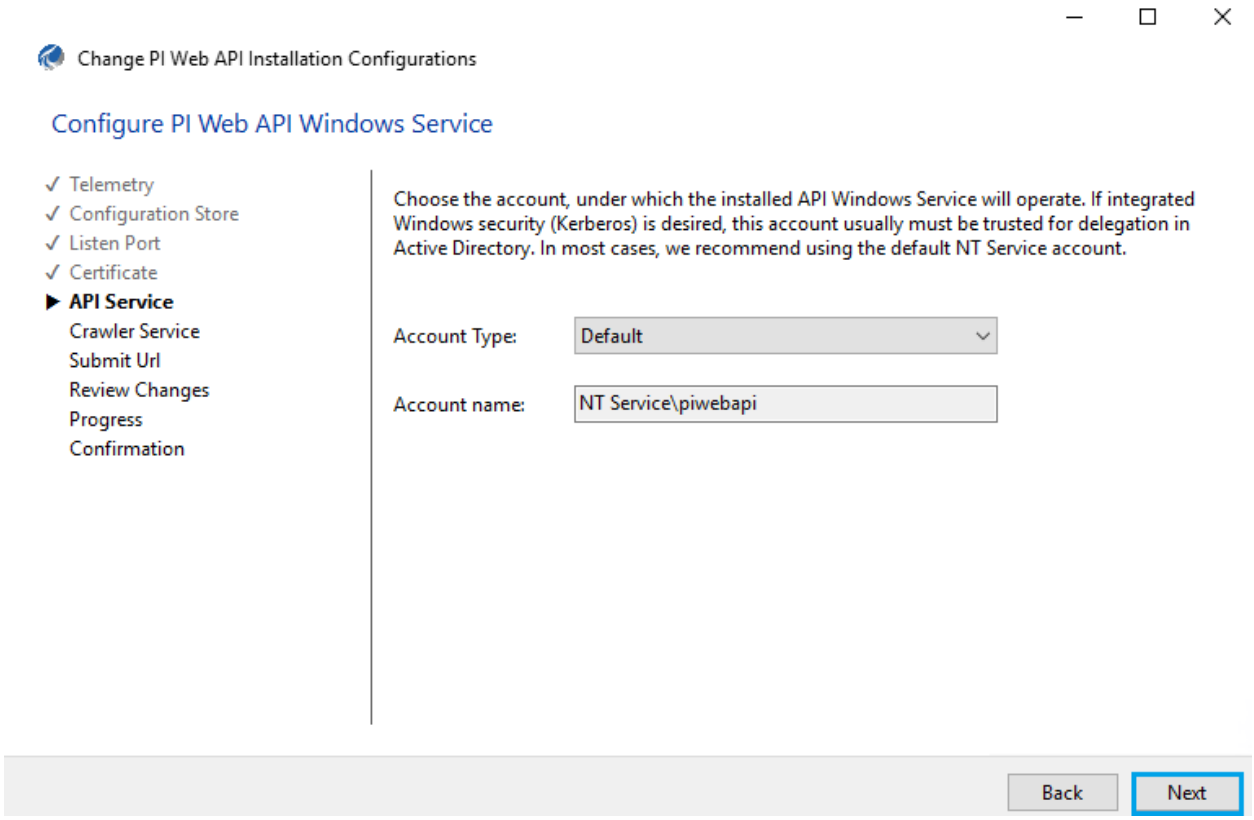
4. Click on **Next**.

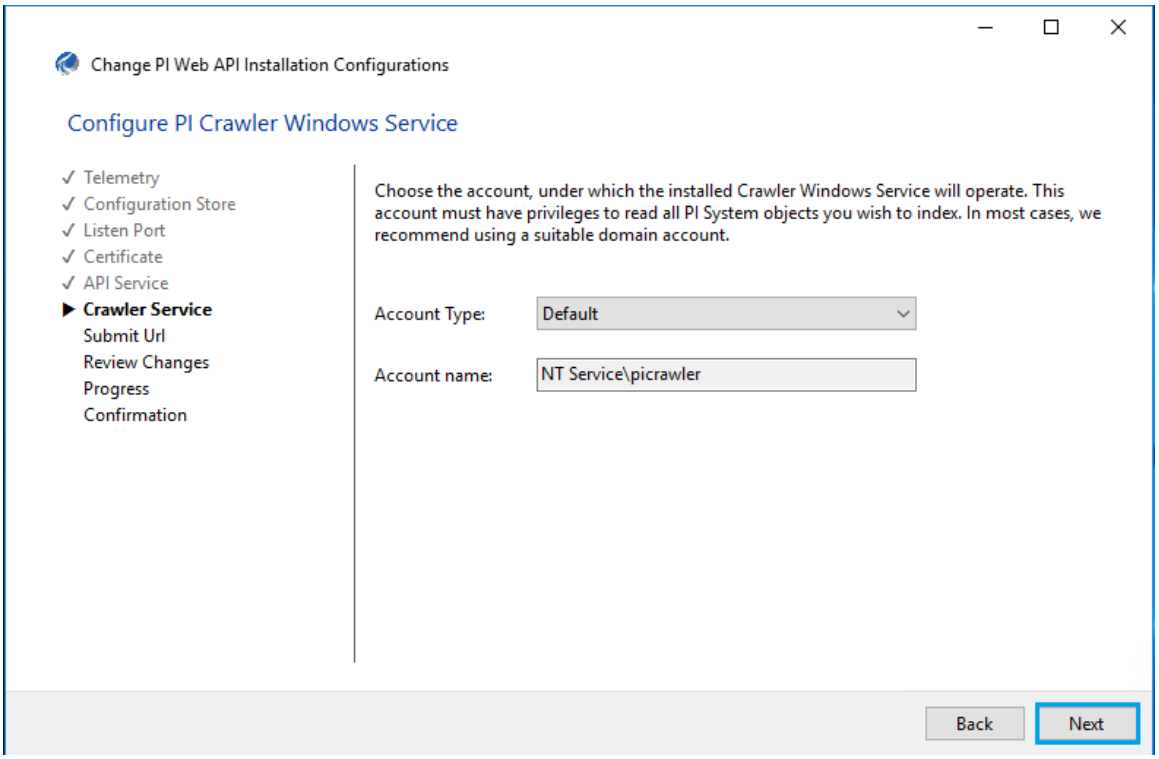


5. Click on **Remove** to remove the certificate and then click on **Yes**.

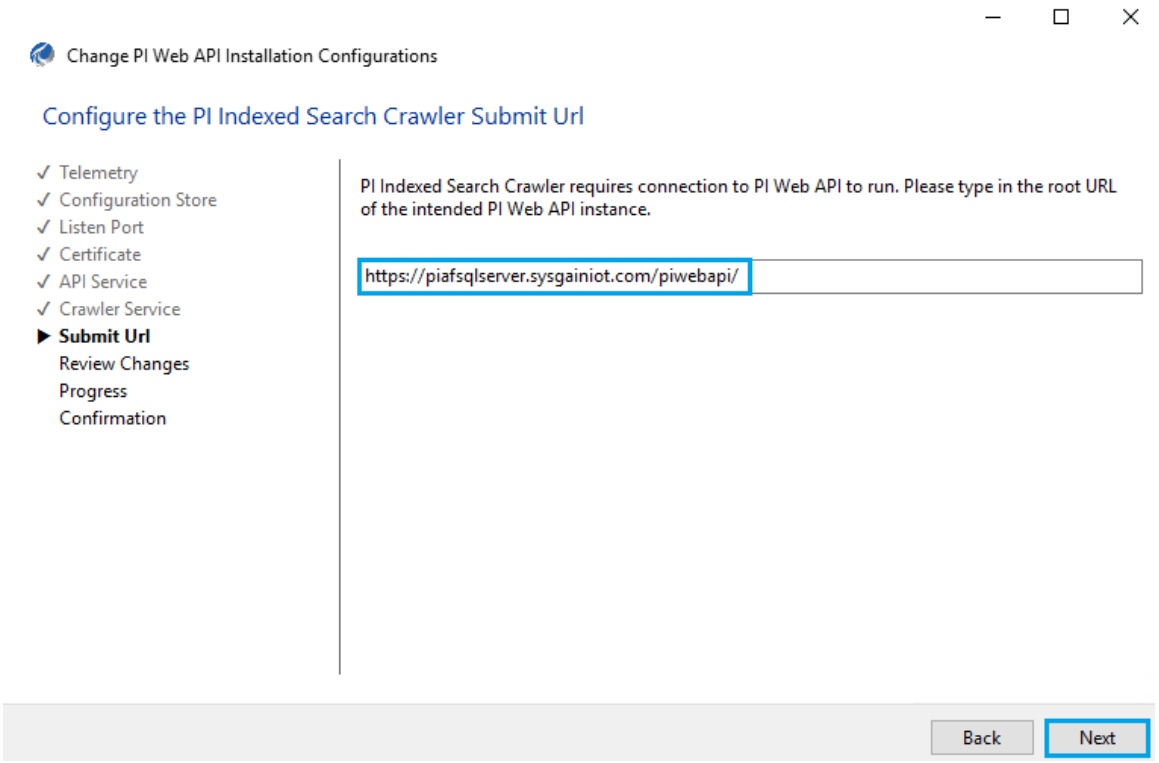


6. Configure **API Service** and **Crawler service** and click **Next**.

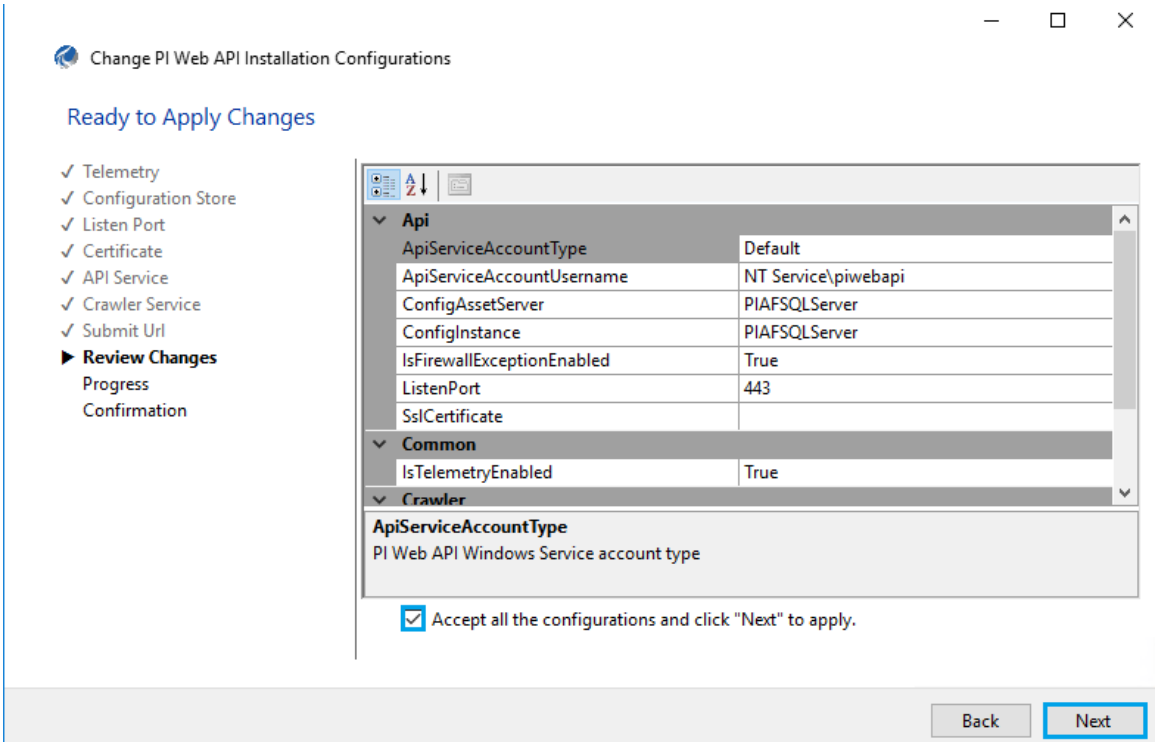


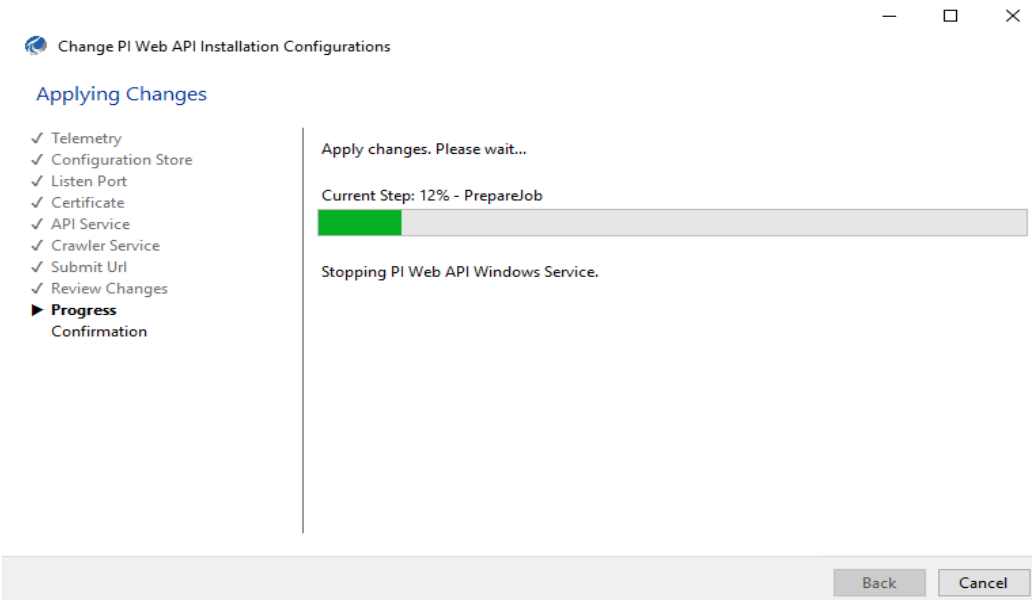


7. Note down the **Submit URL** which will be in later section

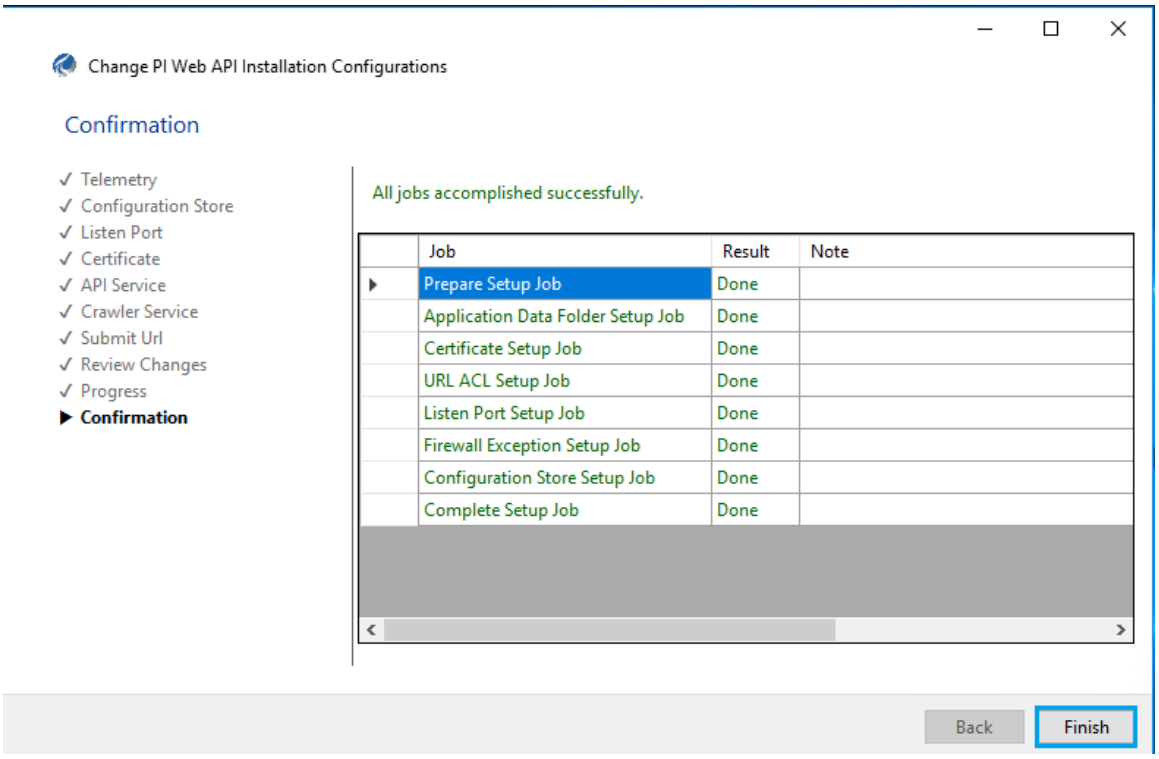


8. Check **Accept all the configurations** and click on **Next**.



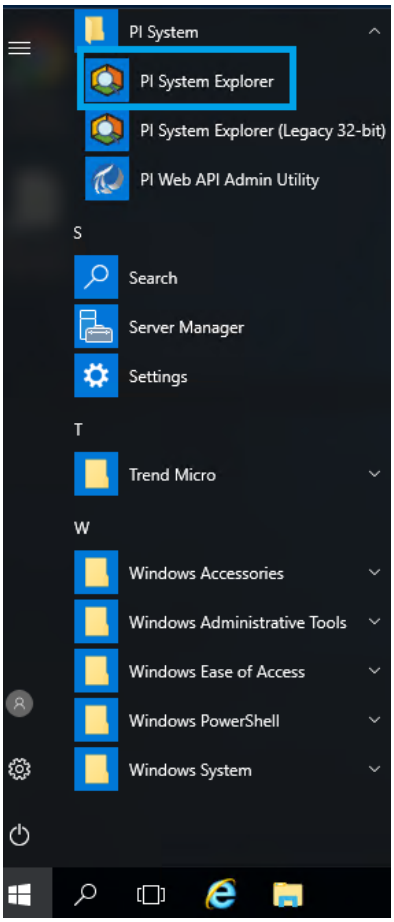


9. Click on **Finish**.

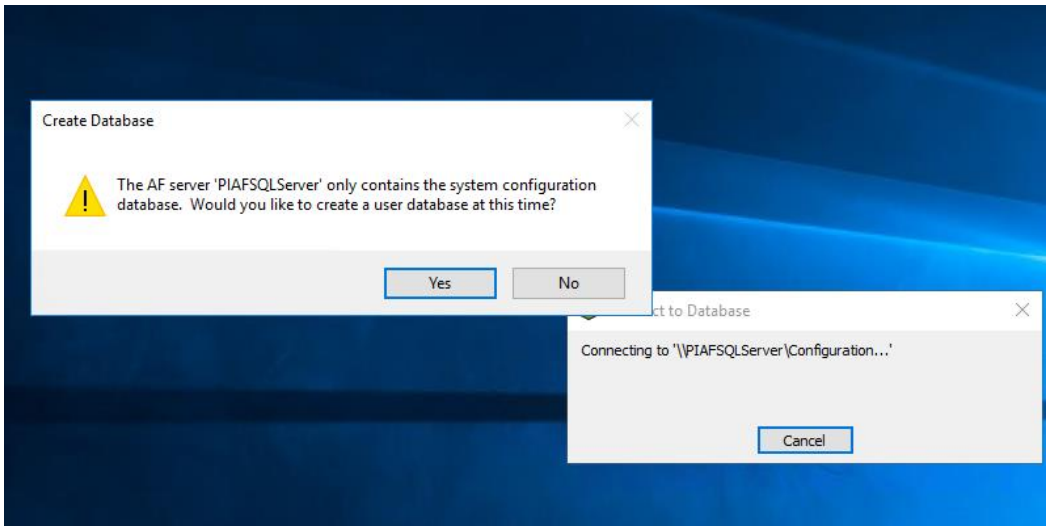


9.4. Creation of Database in PI System Explorer

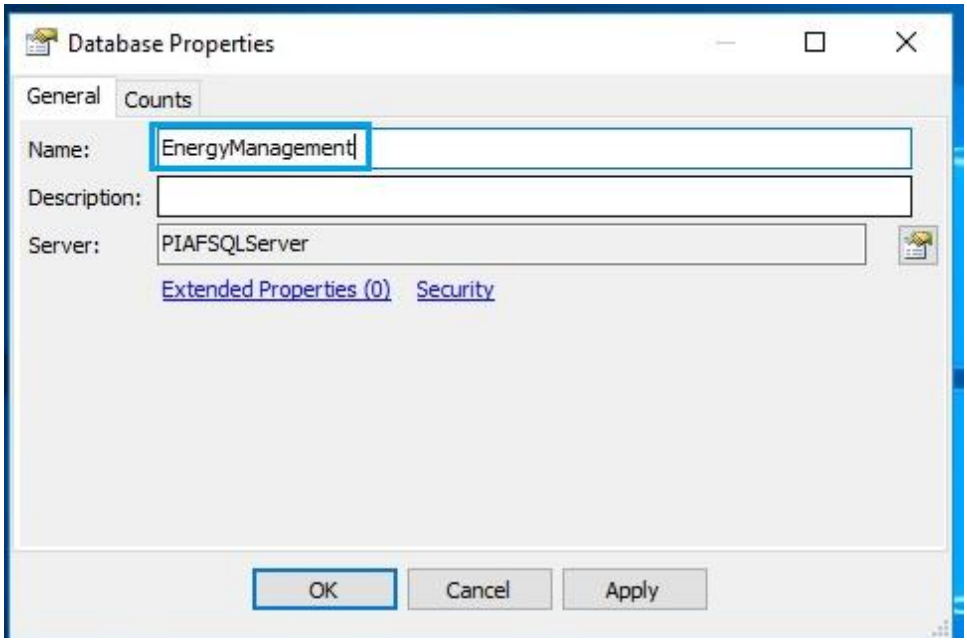
18. On the PIAFSQL machine, Navigate to **PI System Explorer** in PI System folder from the Start menu.


PI System
PI System Explorer
PI System Explorer (Legacy 32-bit)
PI Web API Admin Utility
S
Search
Server Manager
Settings
T
Trend Micro
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows System

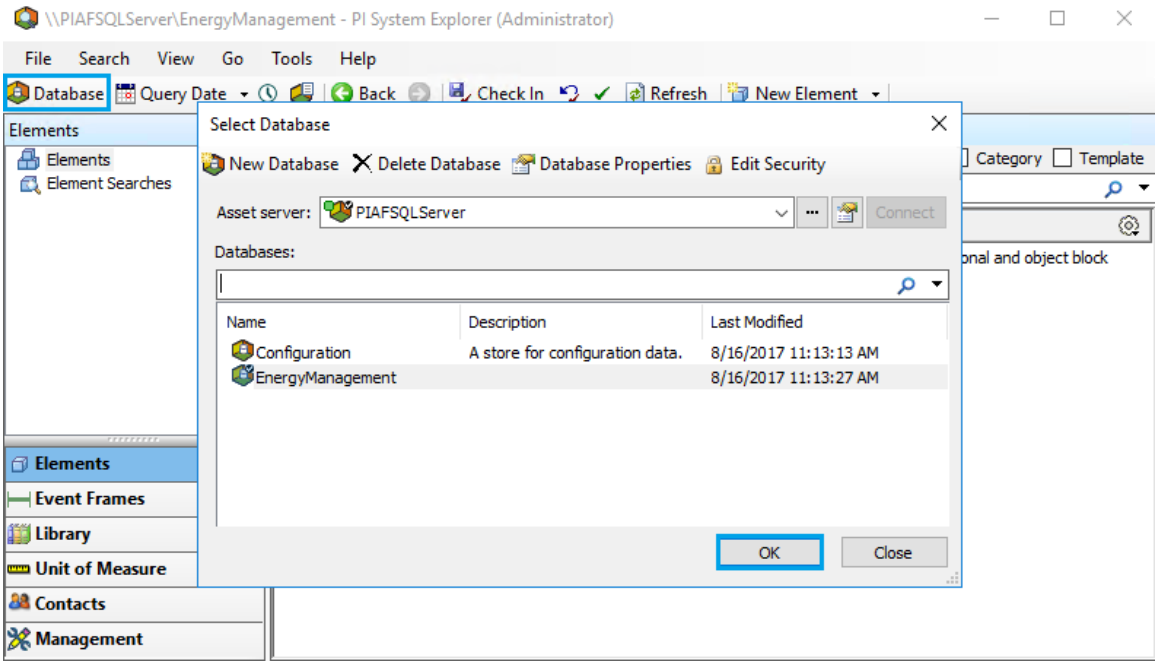
19. Two popups show up, **Connect to Database** and **Create Database.** Click **Yes** on the **Create Database** popup.



20. Enter the Name as **EnergyManagement** in Database properties and click on **OK.** It will create the **EnergyManagement** database in PIAFSQLServer.

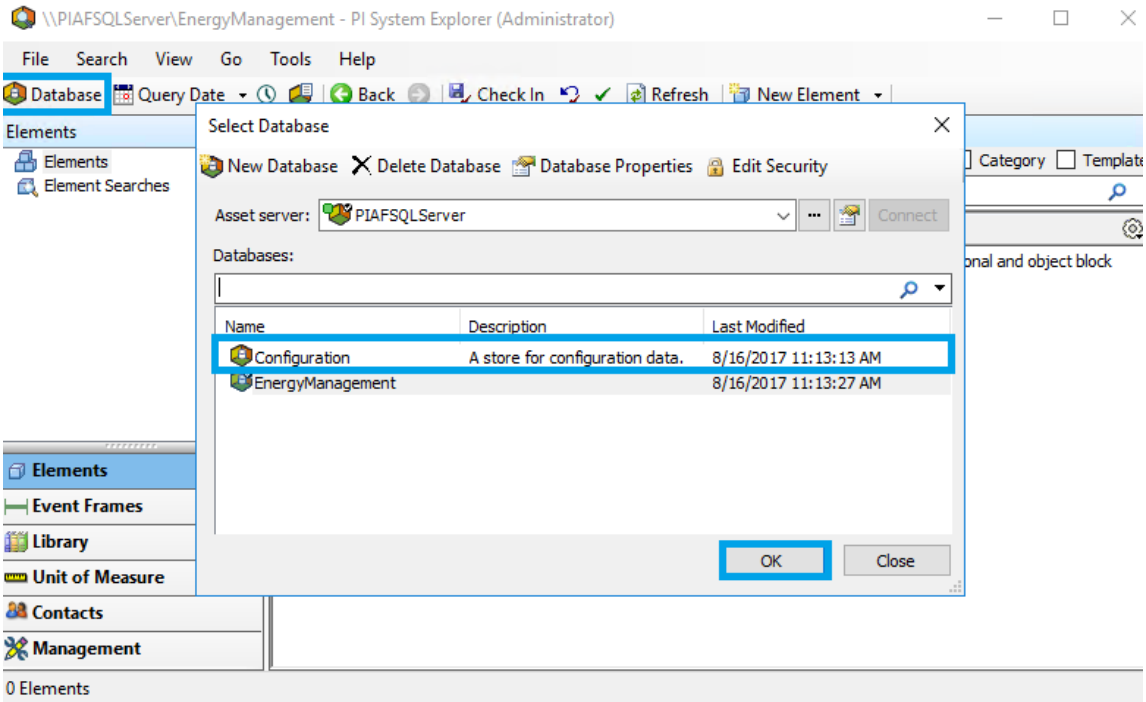


21. Navigate to **PI System Explorer,** click on **Database** to view the created database and click on **OK.**

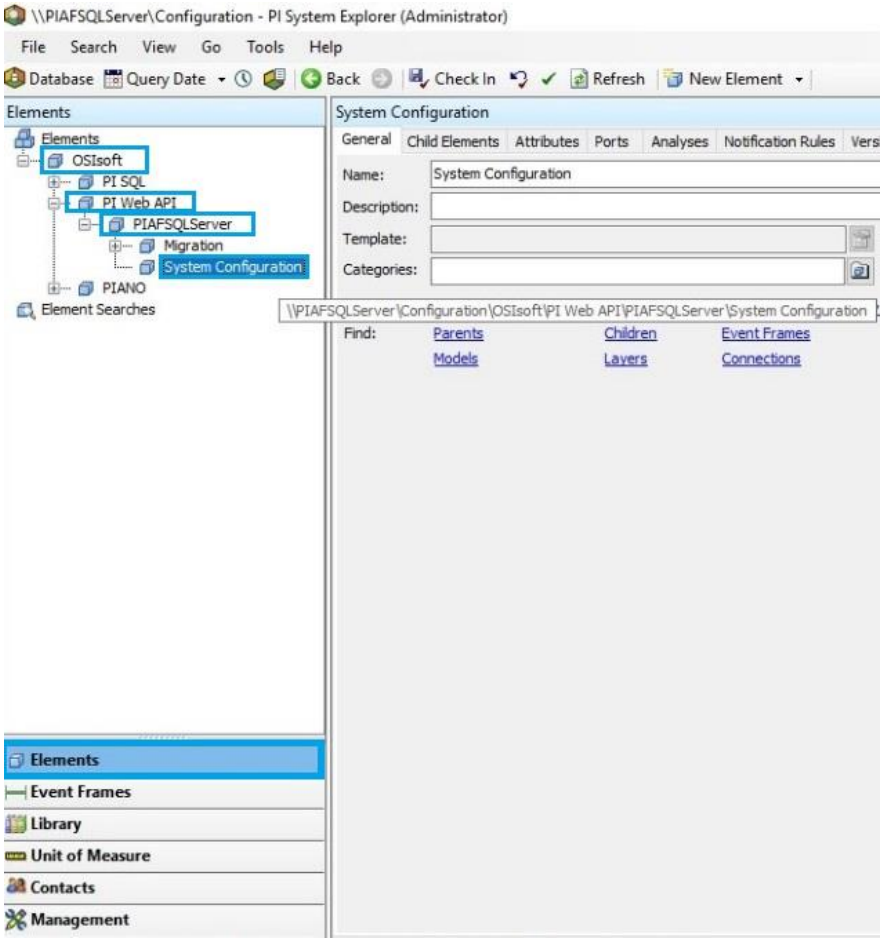


9.5. System Configuration in PI System Explorer

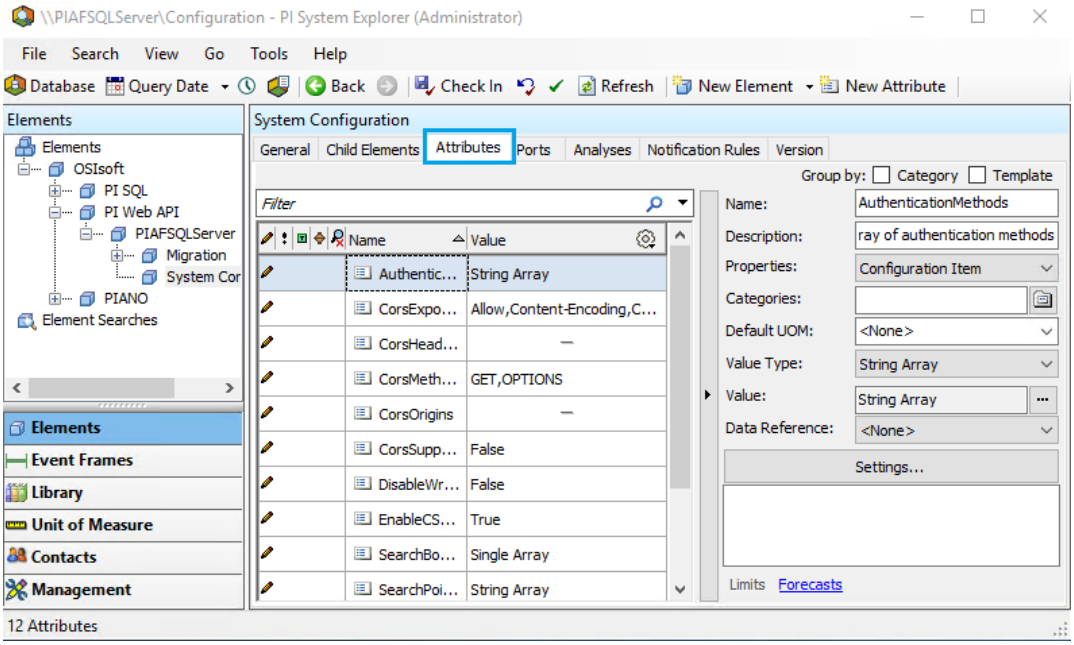
1. Navigate to **PI System Explorer** > Click on **Database** > click **Configuration** under Databases section. Click **OK.**



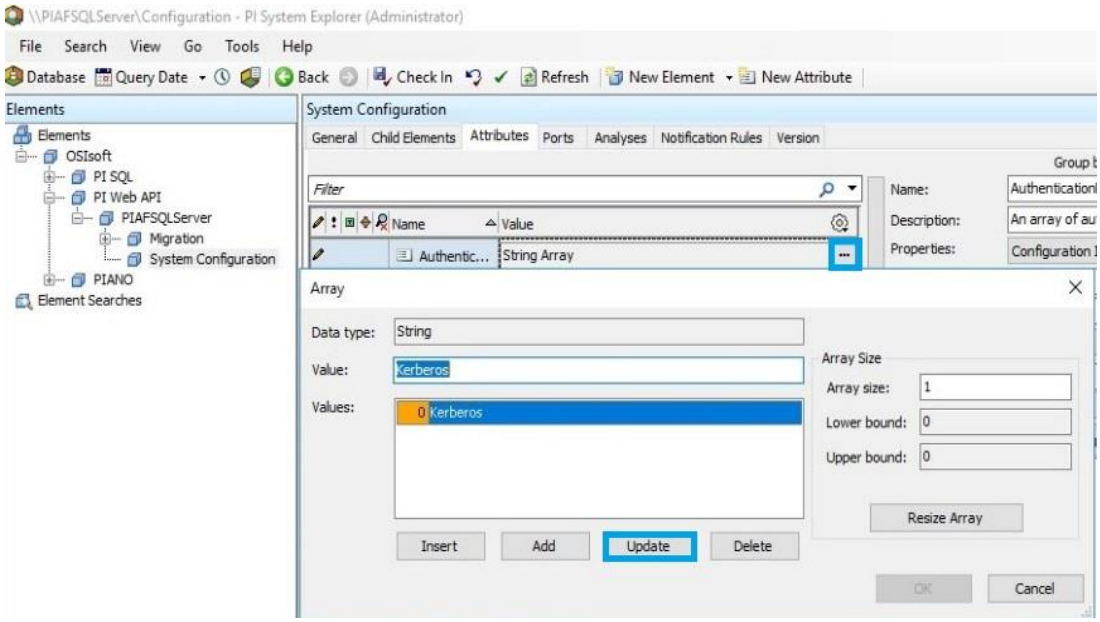
2. Click on **Elements** and navigate to **OSISoft** > **PI Web API** > **PIAFSQLServer** > **System Configuration**.



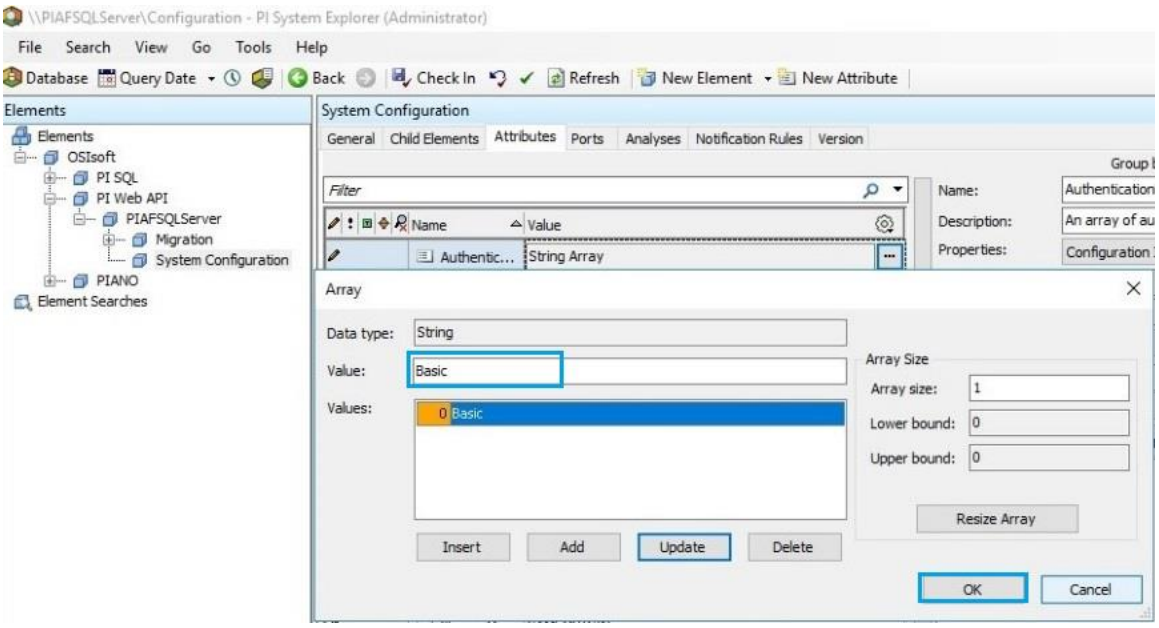
3. Click on **Attributes**.



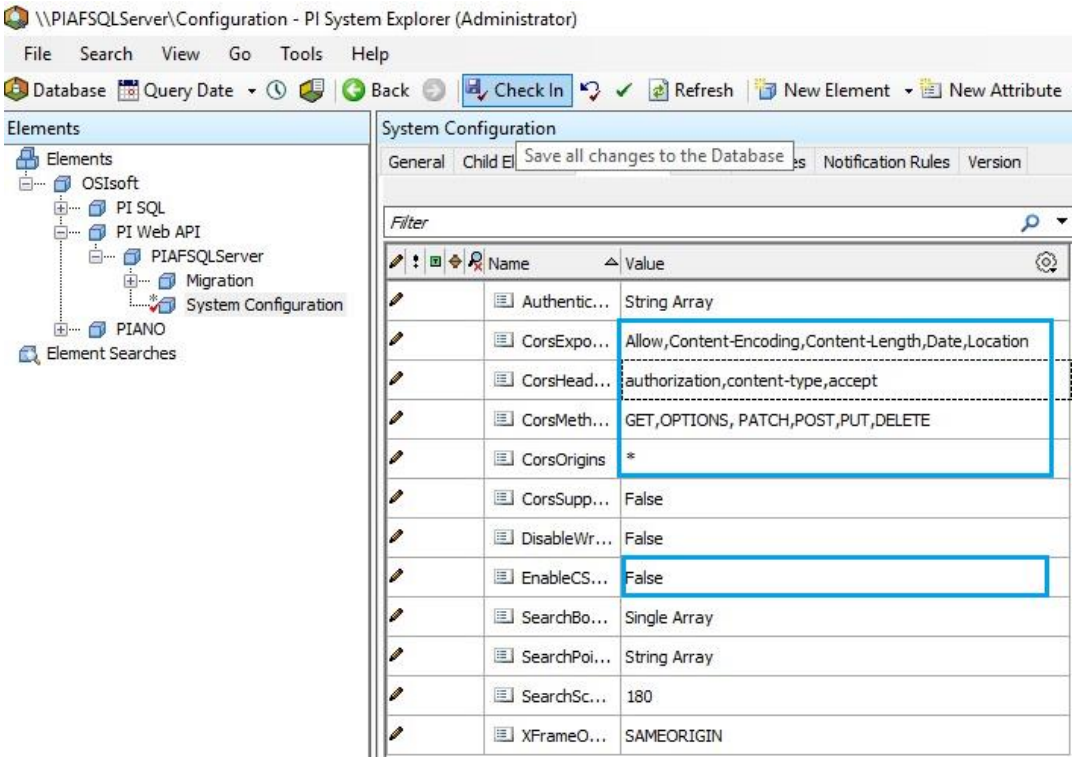
4. Click on **Authentication**, then browse to authentication value and update the value to **Basic** from **Kerberos**.



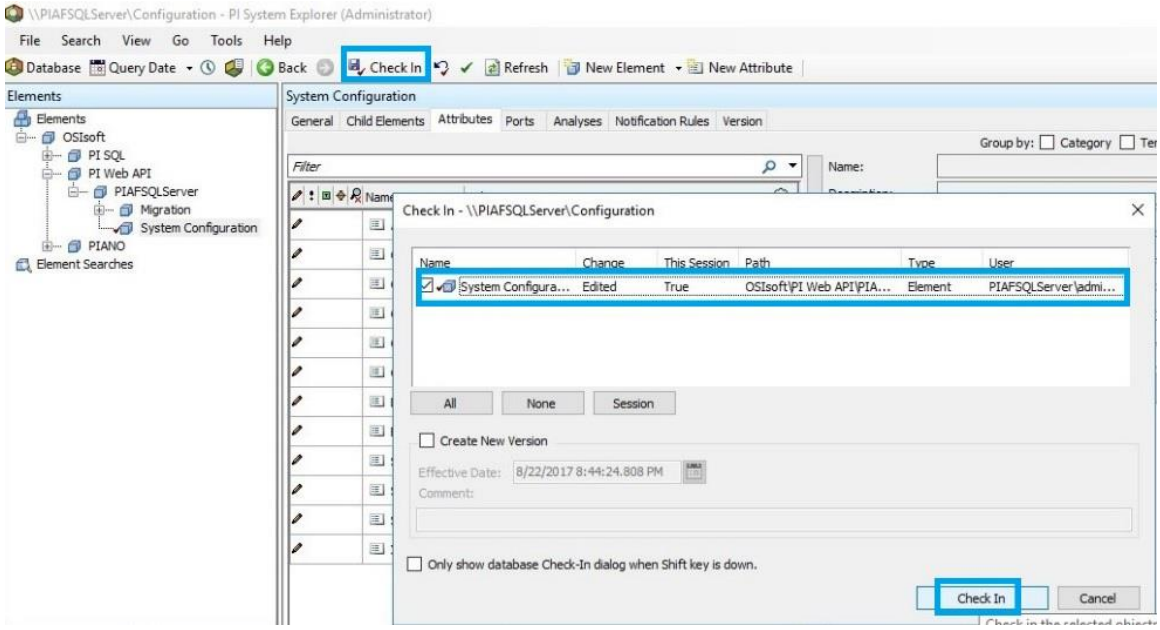
5. Click on **Update**, then **OK**.



6. Similarly, change the following values:
    - EnableCSRFDefense to **False**.
    - Set CorsOrigins as *****
    - Corsmethods as **GET, OPTIONS, PATCH, PUT, POST, DELETE**
    - CorsHeaders as **authorization,content-type,accept**



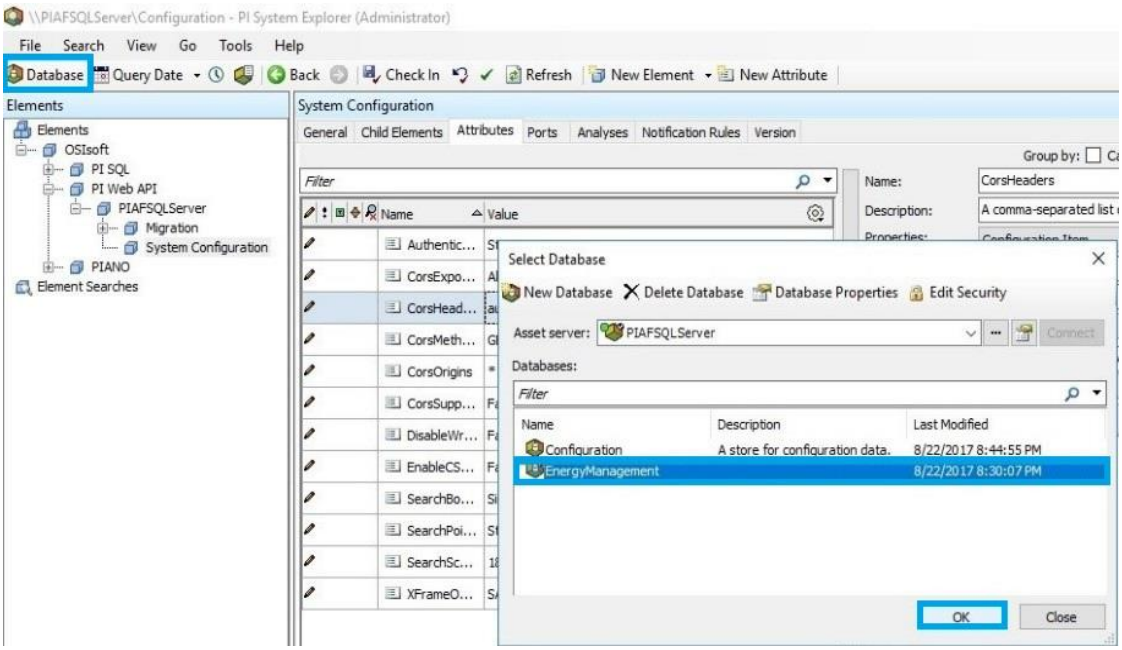
7. Select the **System Configuration** again and click on **Check In**.



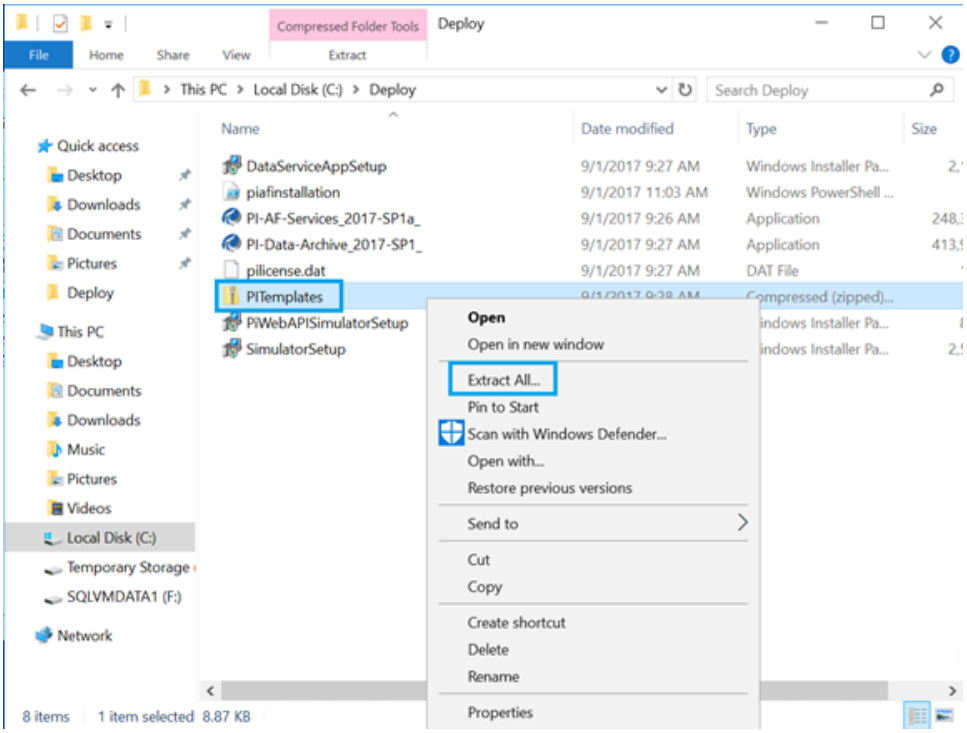
9.6. Import .XML Files into AF Server

1. From the Bastion host connect to the **PIAFSQLServer** virtual machine through the private address with the credentials provided in the output section.

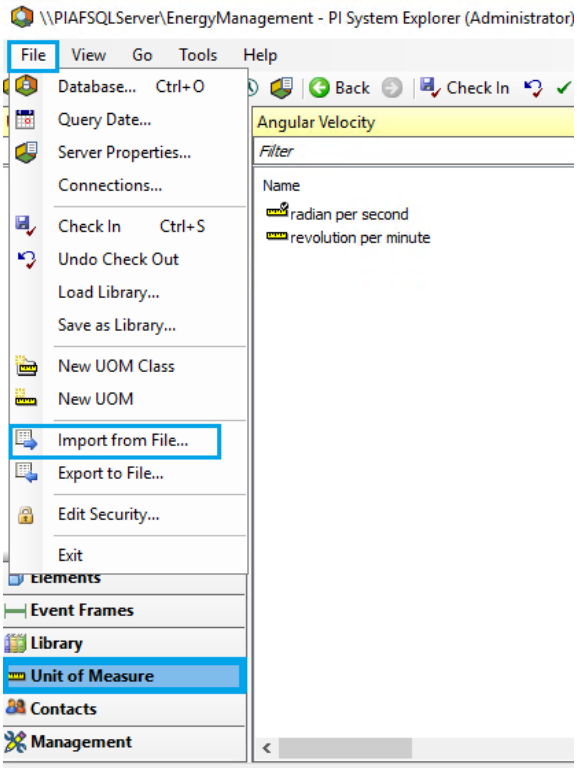
2. Navigate to **PI System Explorer > Select Database > Click on Energy Management** > Click on **OK**.



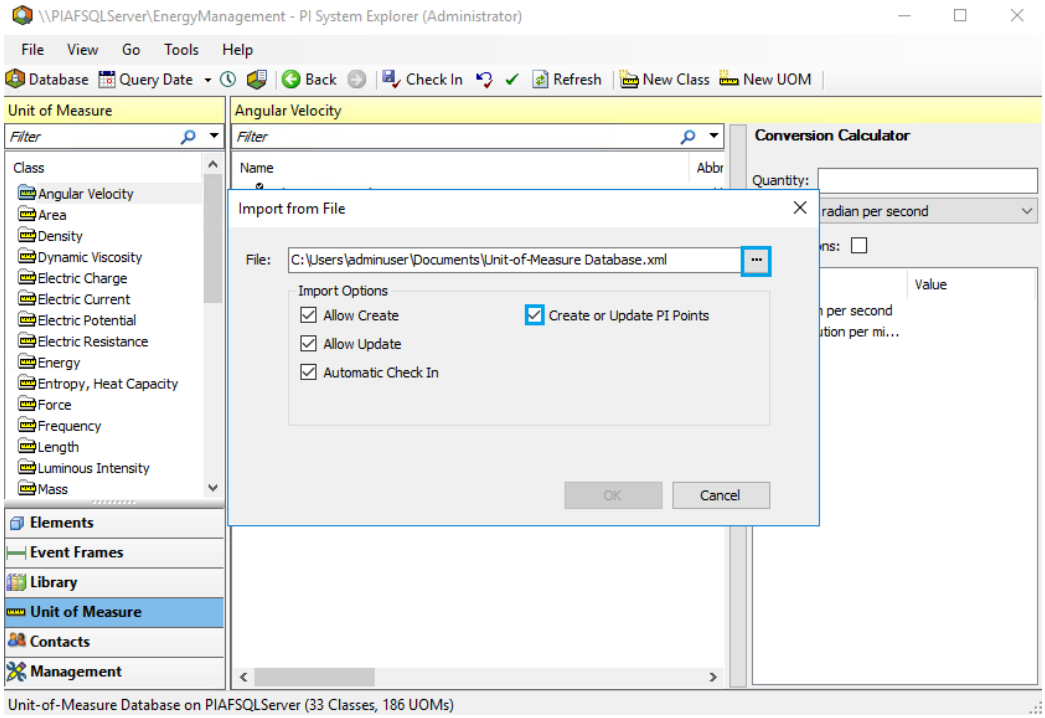
3. Navigate to **Local disk (C:) > Deploy >** unzip **PI templates.**



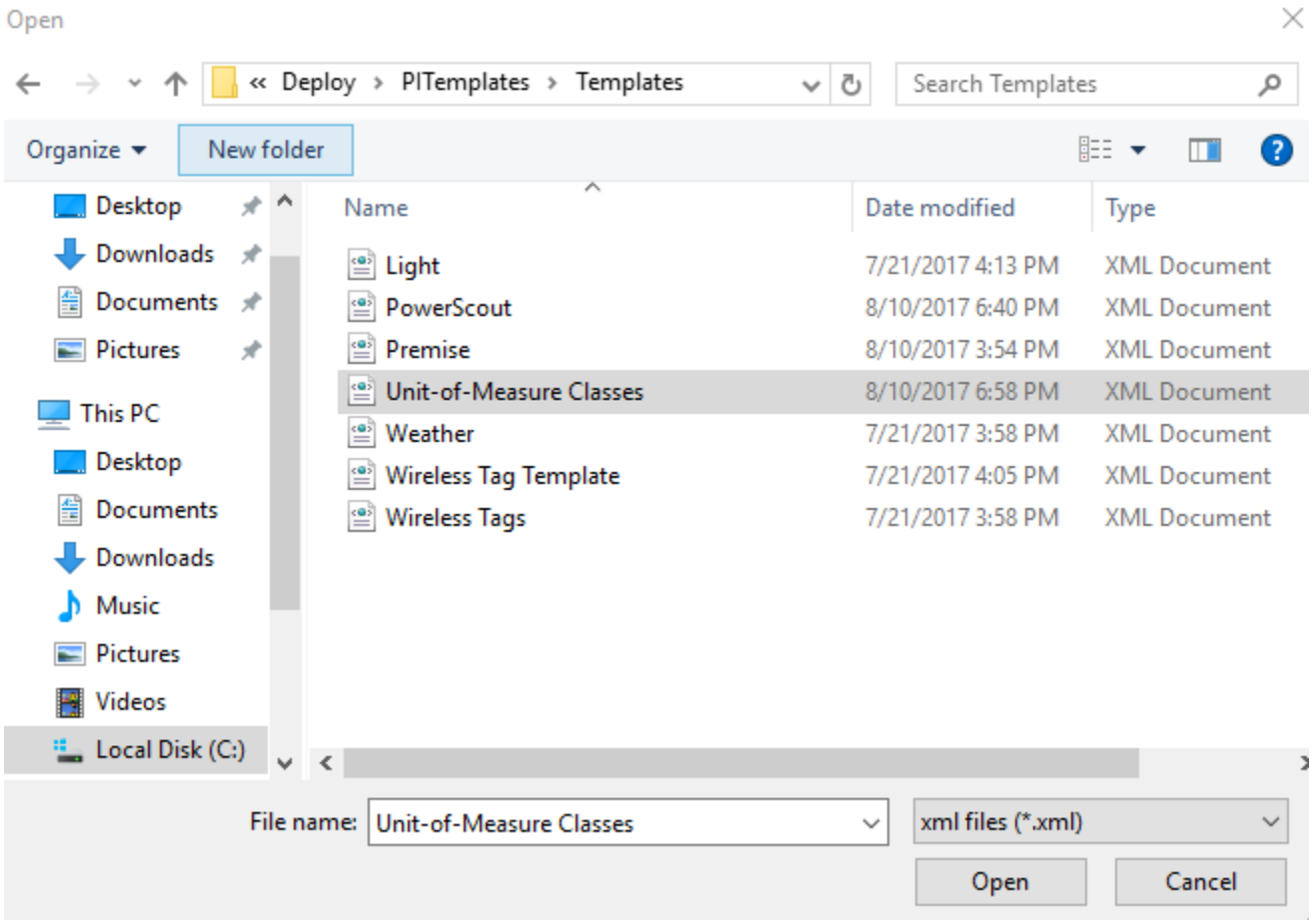
4. Select **Unit of Measure > File > Import from file**



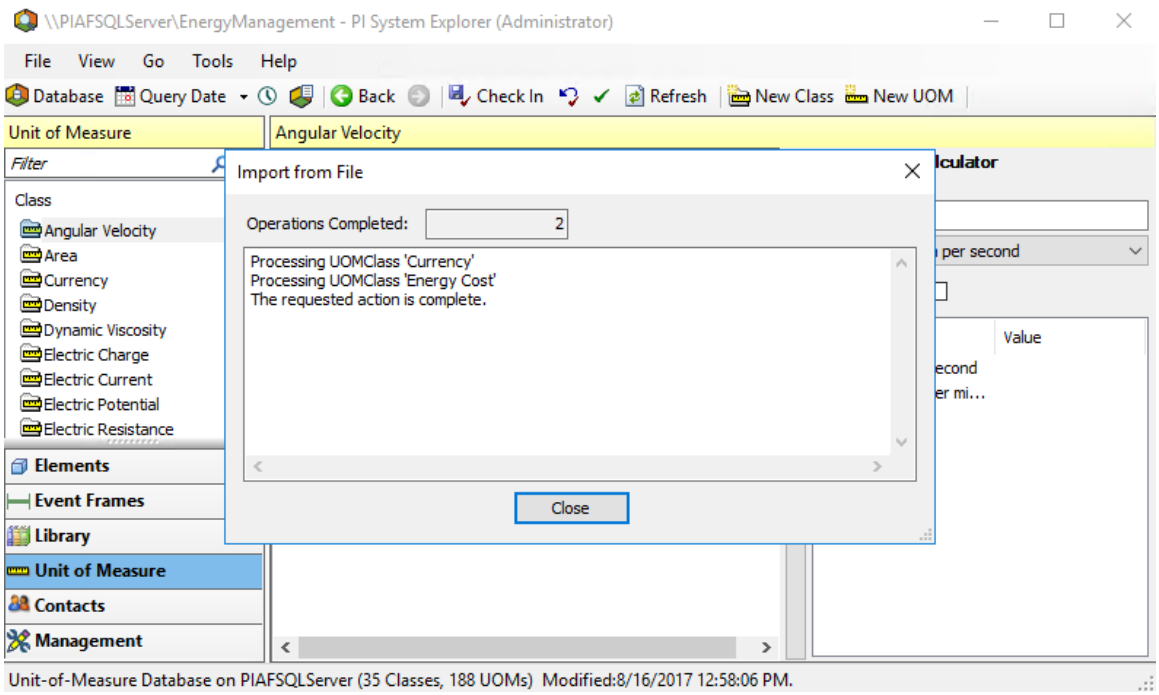
5. Check the box for **Create or Update the PI Points** > browse to **local disk (C:)** > **Deploy** > **PITemplates** > Select **Unit of Measure Classes** > Click on **Open.**



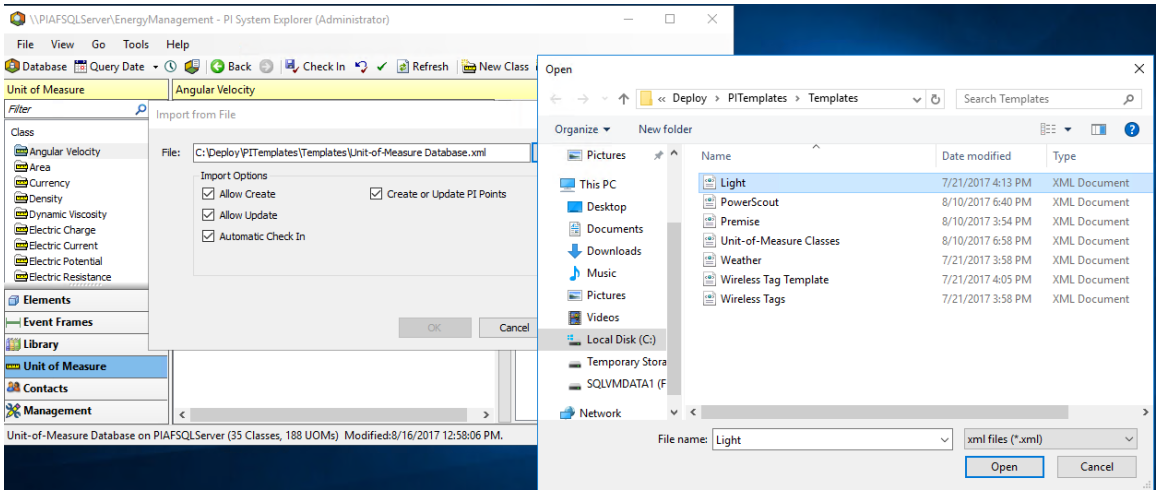
After Open click on ok.



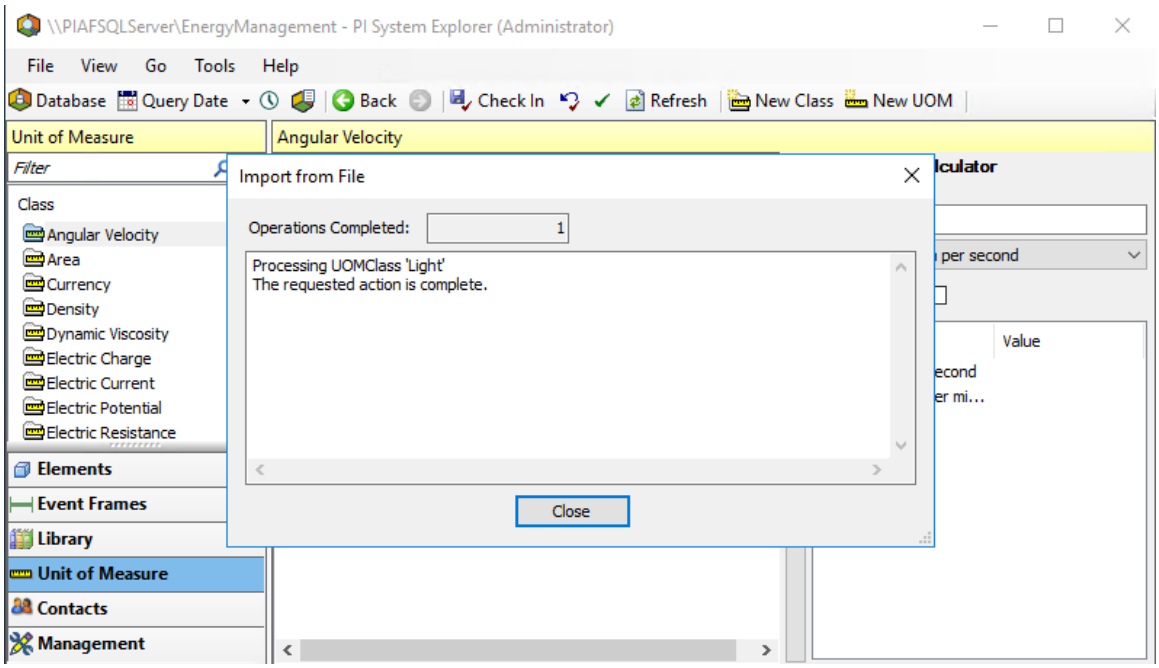
6. You can find the status of the completed operation. Click on **Close**.



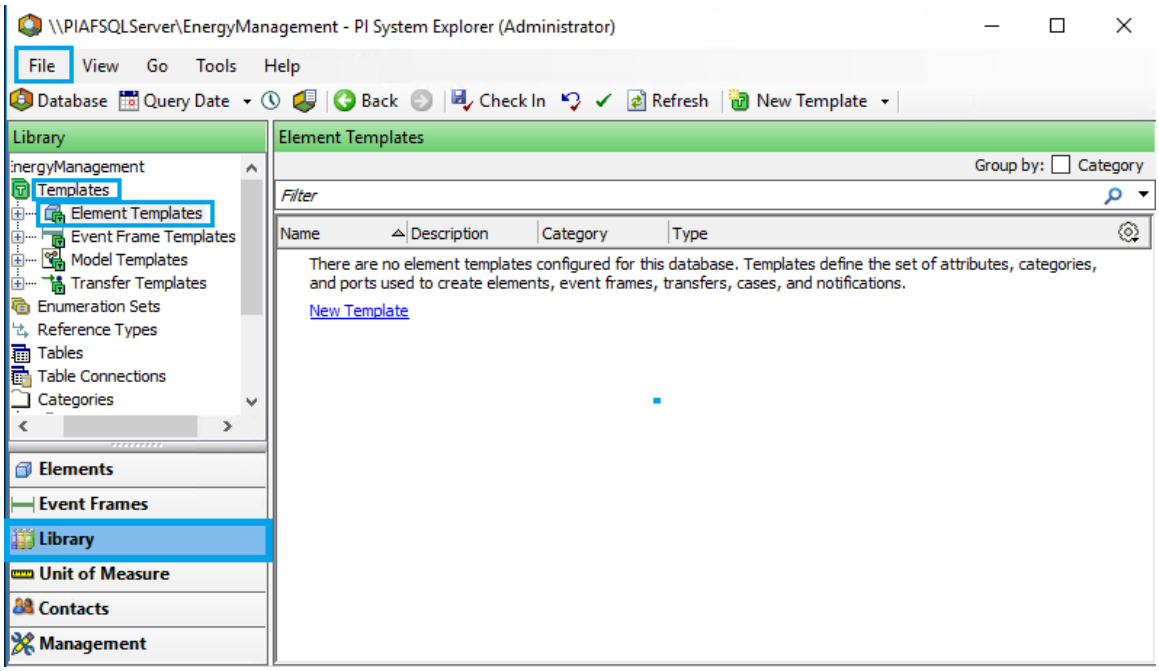
7. Again click on the import from file from file menu Check the box **Create or Update the PI Points >** browse to **C:\Deploy\PITemplates >** Select **Light** and click on **Open**.



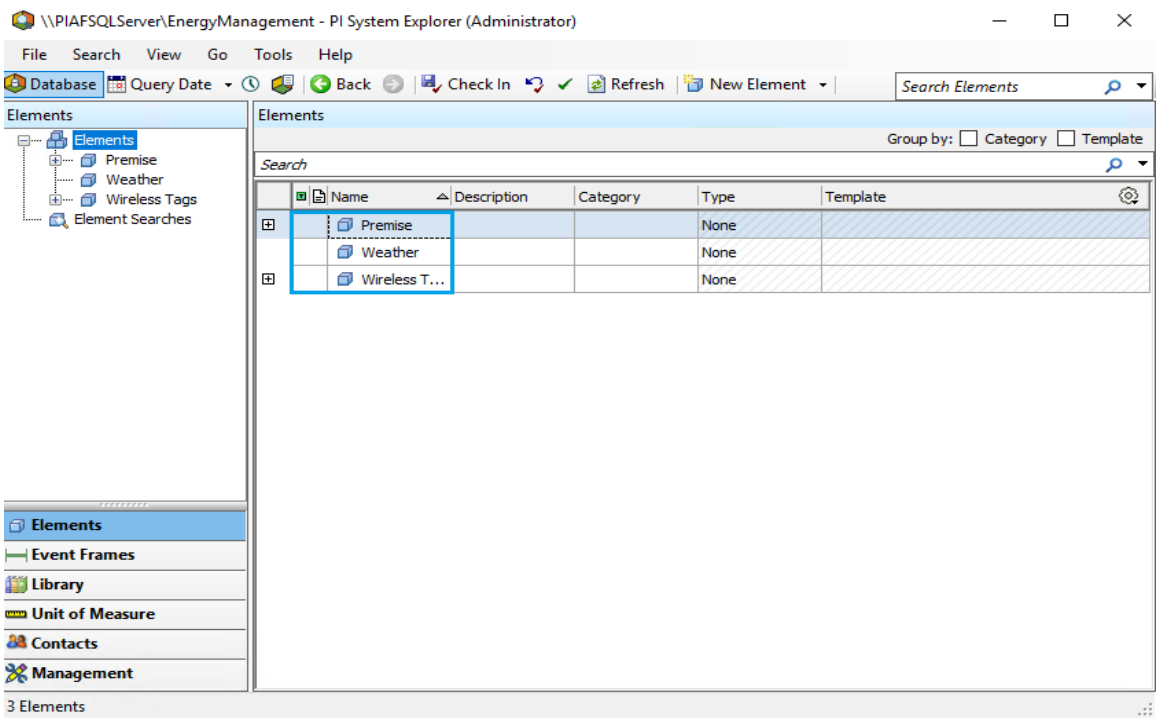
8. You can see the status of the completed operations. Click on **Close**.


\\PIAFSQLServer\EnergyManagement - PI System Explorer (Administrator)
File View Go Tools Help
Database Query Date Back Check In Refresh New Class New UOM
Unit of Measure
Angular Velocity
Filter
Class
Angular Velocity
Area
Currency
Density
Dynamic Viscosity
Electric Charge
Electric Current
Electric Potential
Electric Resistance
Elements
Event Frames
Library
Unit of Measure
Contacts
Management
Import from File
Operations Completed: 1
Processing UOMClass 'Light'
The requested action is complete.
Close
per second
Value

9. Similarly Select **Library > Templates > Element Templates.** Click on **File > Import from file** (File location – C:\Deploy\PITemplates\Templates) import the below two files.
   - Powerscout
   - Wireless Tag Template

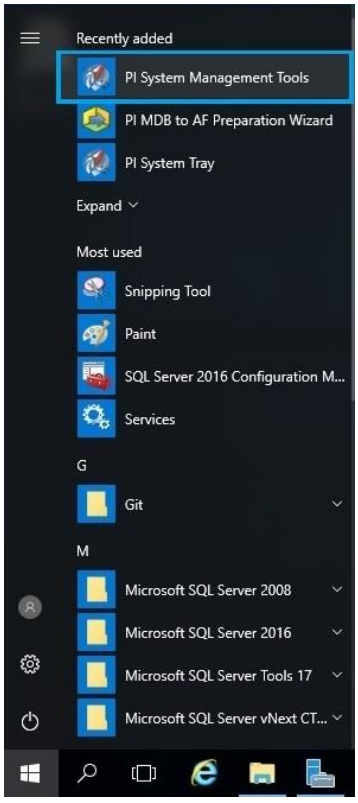


10. Similarly Select **Elements > Import File** (File location – C:\Deploy\PITemplates\Templates) imported the below three files.
    - Weather
    - Premise
    - Wireless Tags

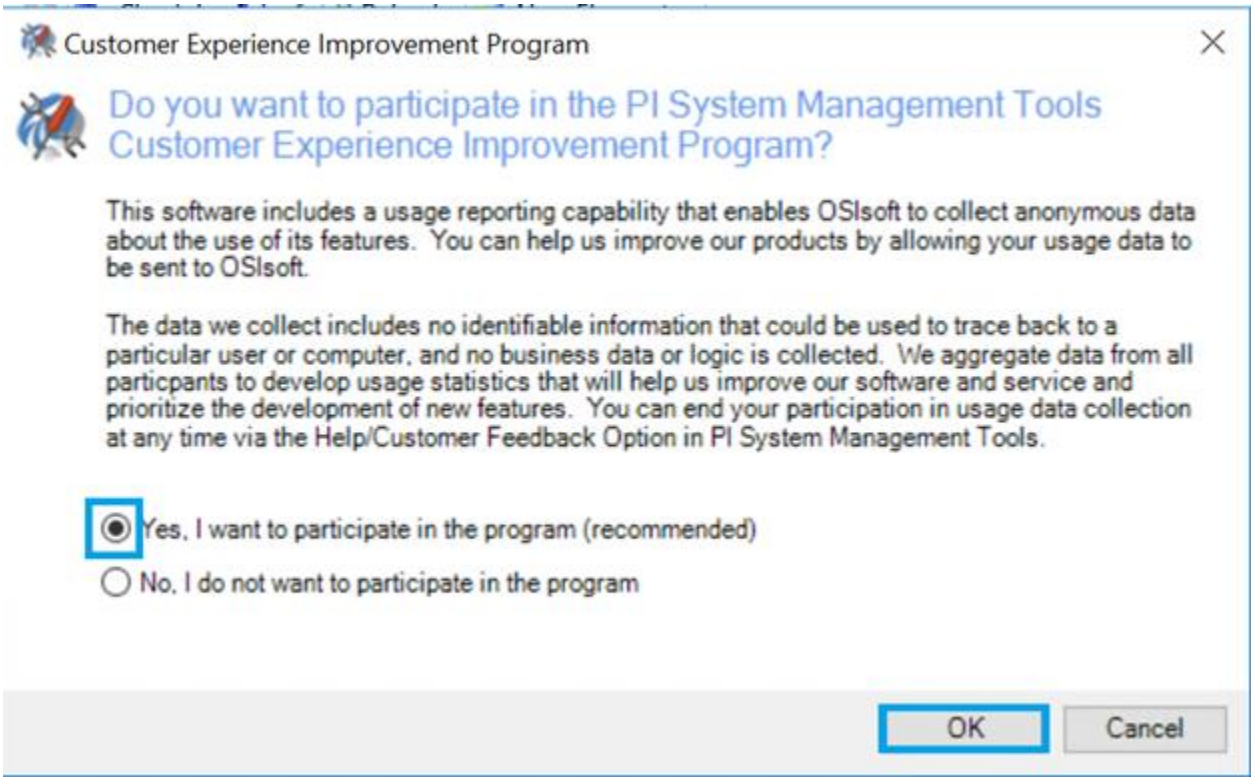

\\PIAFSQLServer\EnergyManagement - PI System Explorer (Administrator)
File
Search
View
Go
Tools
Help
Database
Query Date
Back
Check In
Refresh
New Element
Search Elements
Elements
Elements
Premise
Weather
Wireless Tags
Element Searches
Elements
Group by:
Category
Template
Search
Name
Description
Category
Type
Template
Premise
None
Weather
None
Wireless T...
None
Elements
Event Frames
Library
Unit of Measure
Contacts
Management
3 Elements

9.7. Update Security in PI System Management Tools

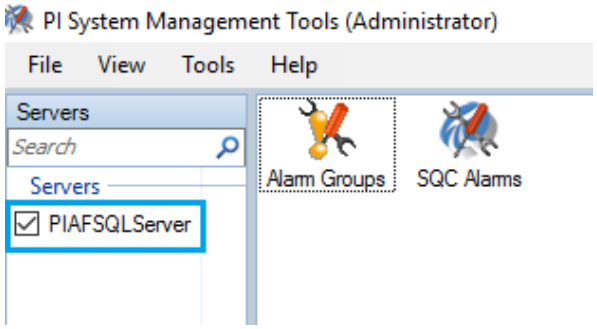
1. From the Start menu, open the **PI System Management Tools**.



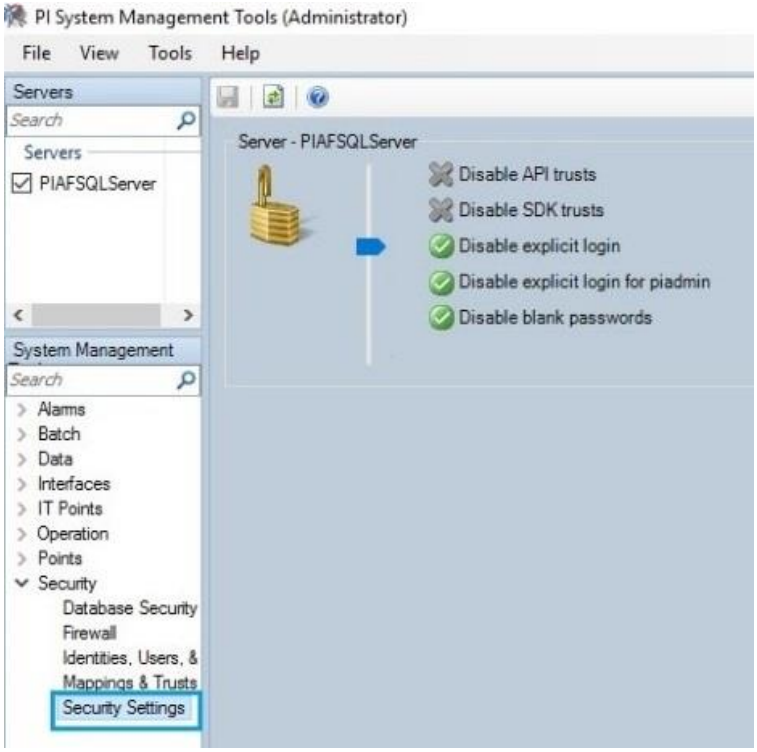
2. Check in the box Yes, I want to participate and click on **OK**



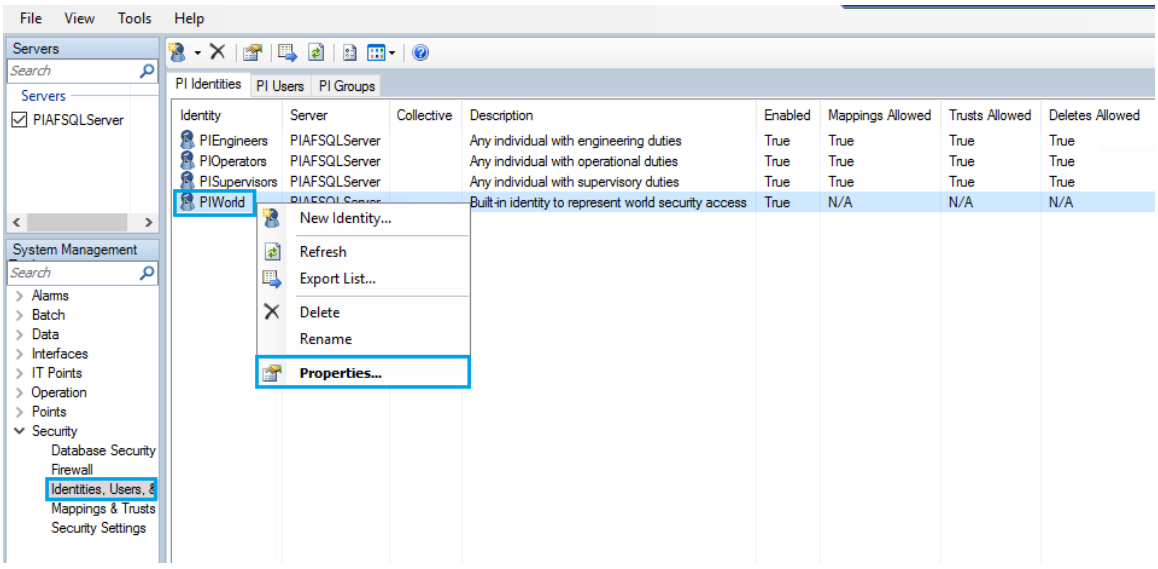
3. Under Servers, check the **PIAFSQLServer** box.



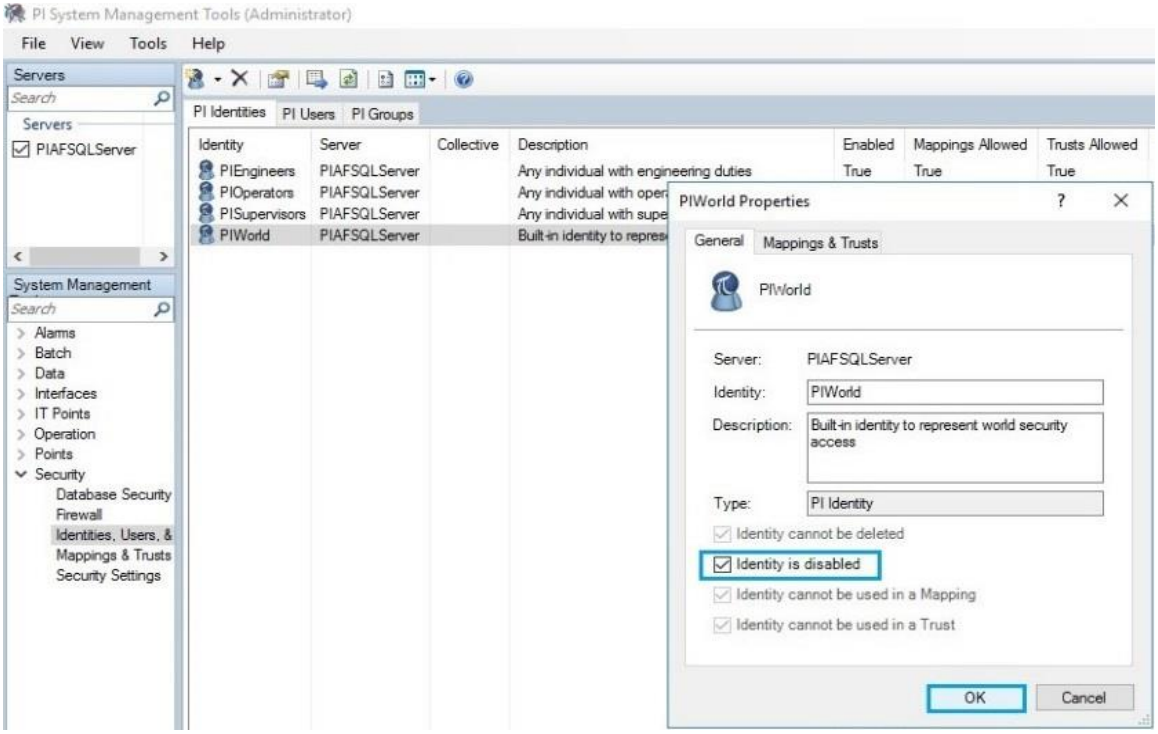
4. Click on **Security** under **System Management**, then click on **Security Settings**.



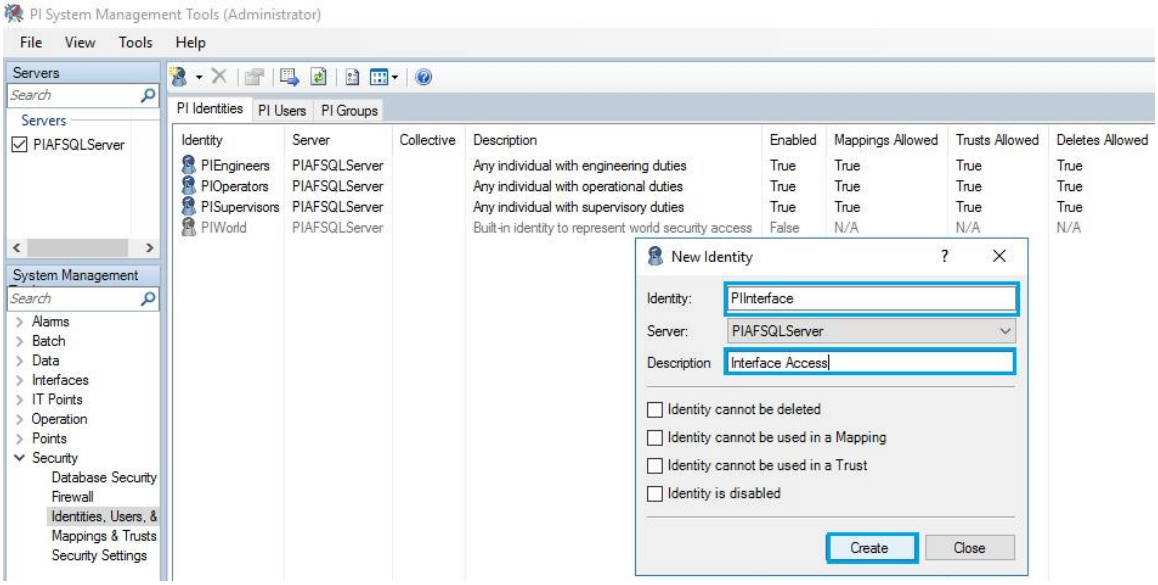
5. Click on **Identities**, **Users and Groups**, then right-click on **PIWorld** under PI identities and select **Properties**.



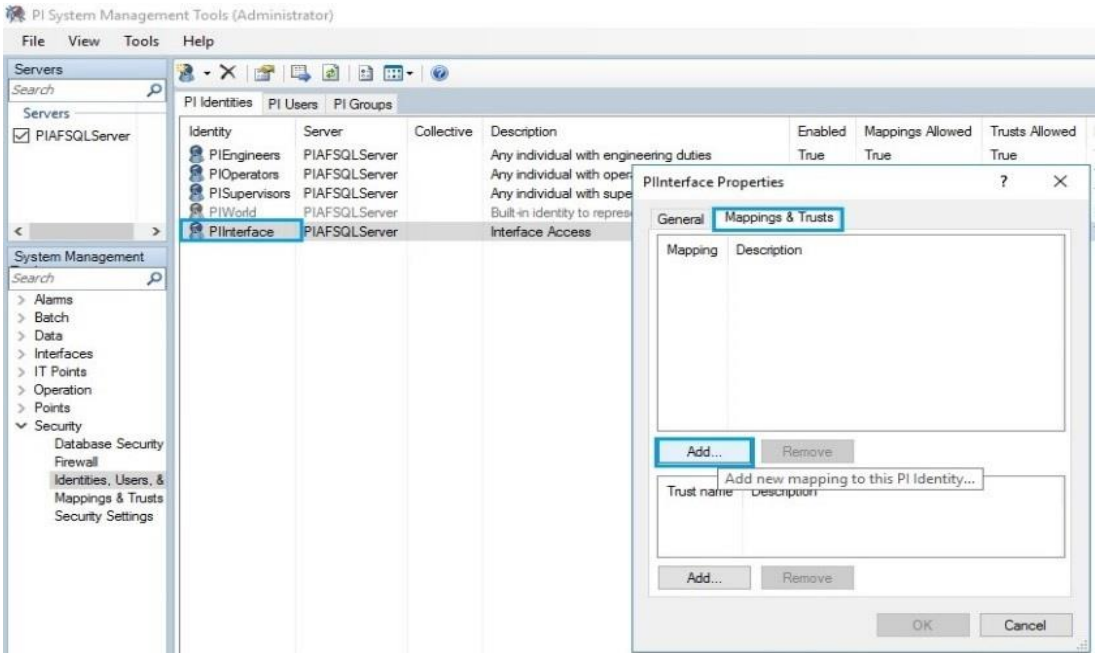
6. Select the **Identity is disabled** checkbox and click on **OK**.



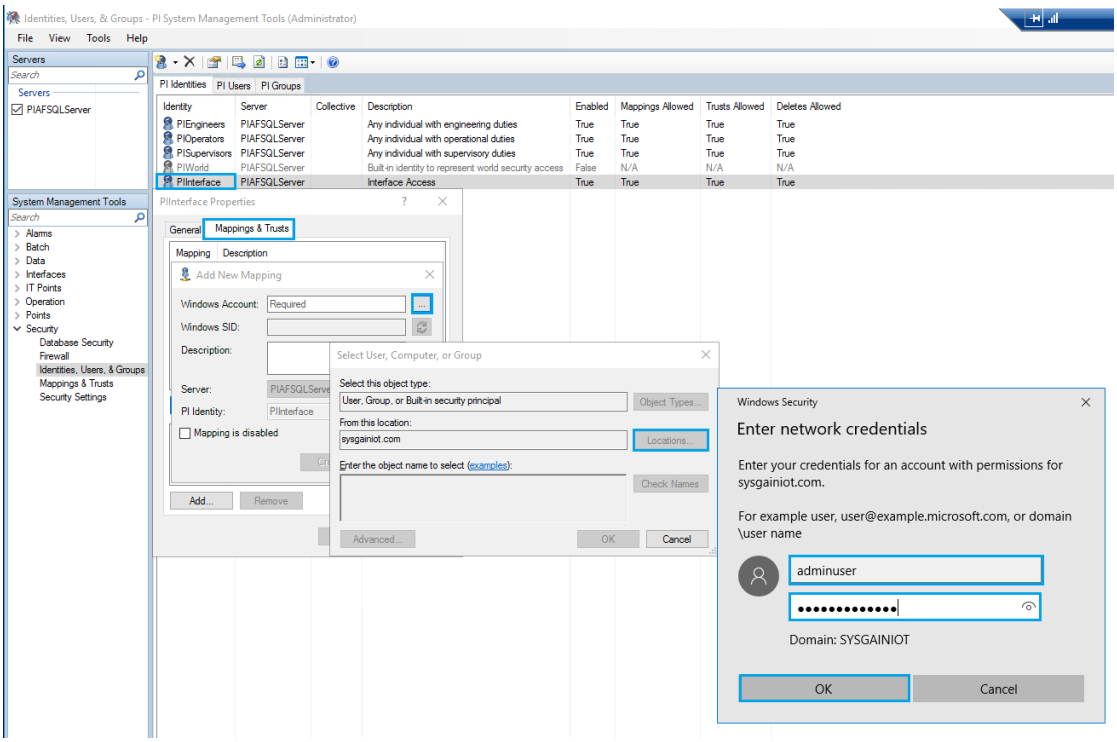
7. The **Enabled** column under **PIWorld** will appear as **False**.
8. Right-click **PI Identities** to create a new identity. Give the identity the name **PIInterface** and the description **Interface Access**, then click on **Create**.



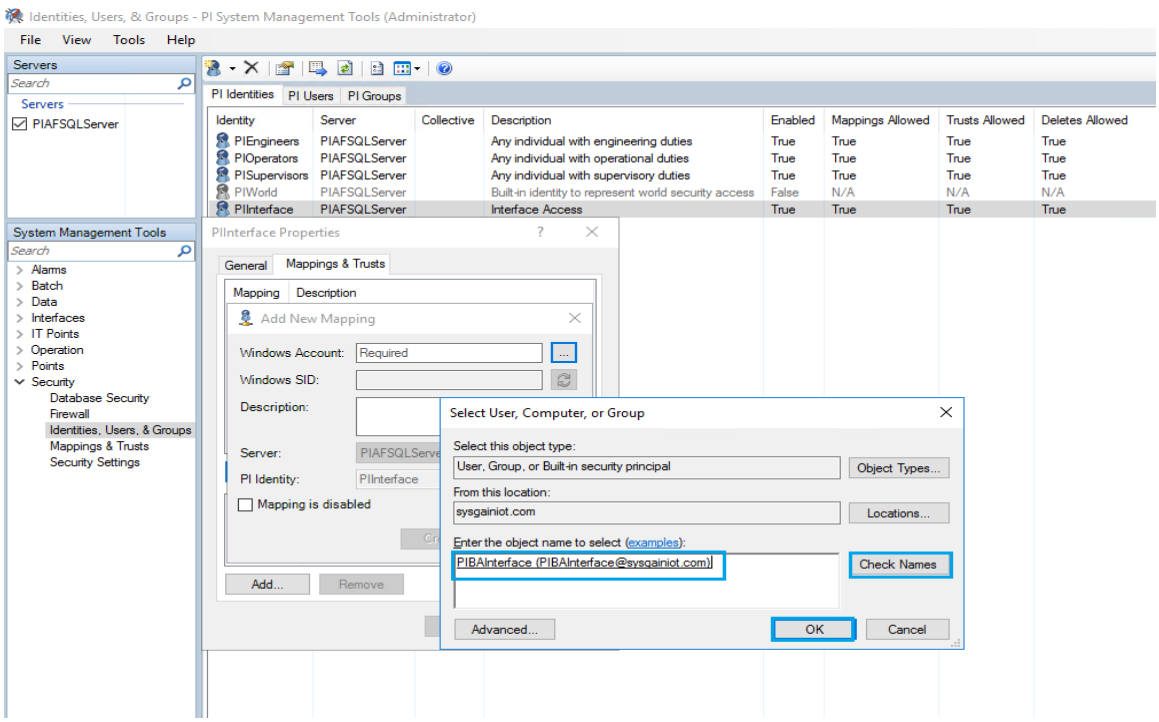
9. Right-click on the newly created **PIInterface** identity, then go to **Properties** > **Mappings & Trusts**, then click on **Add.**



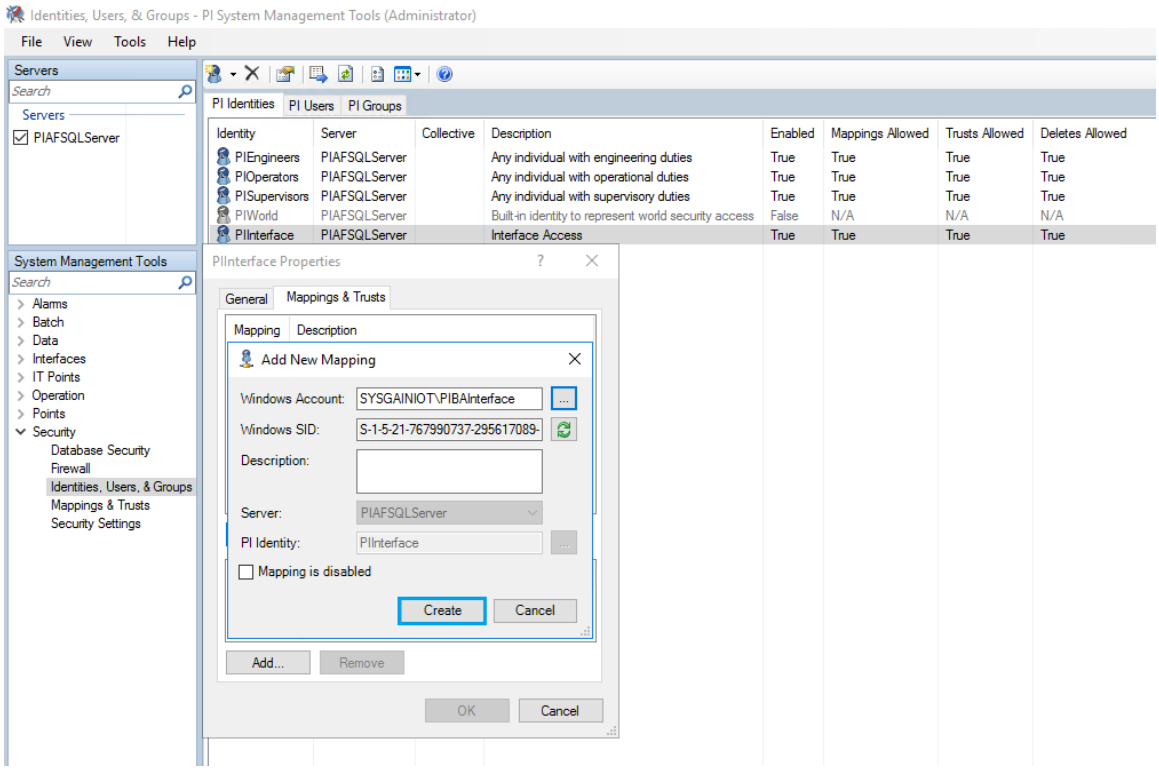
10. After click on **Add** it will show the popup box Add new mapping in that **Browse** at end of **Windows Account** again it will show the popup box as select user,computer,or group in that click on **Locations**. select the domainname Enter the credentials and click on **OK**



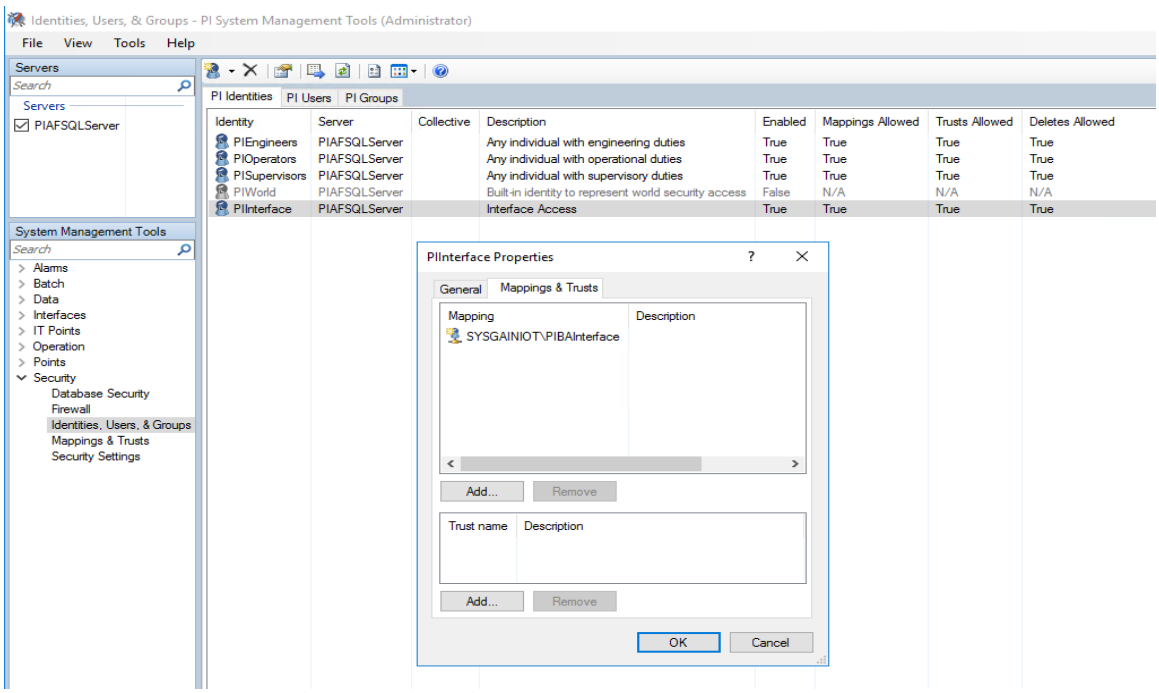
11. Give object name as **PIBAInterface** > **Click on Check Names** > **OK**



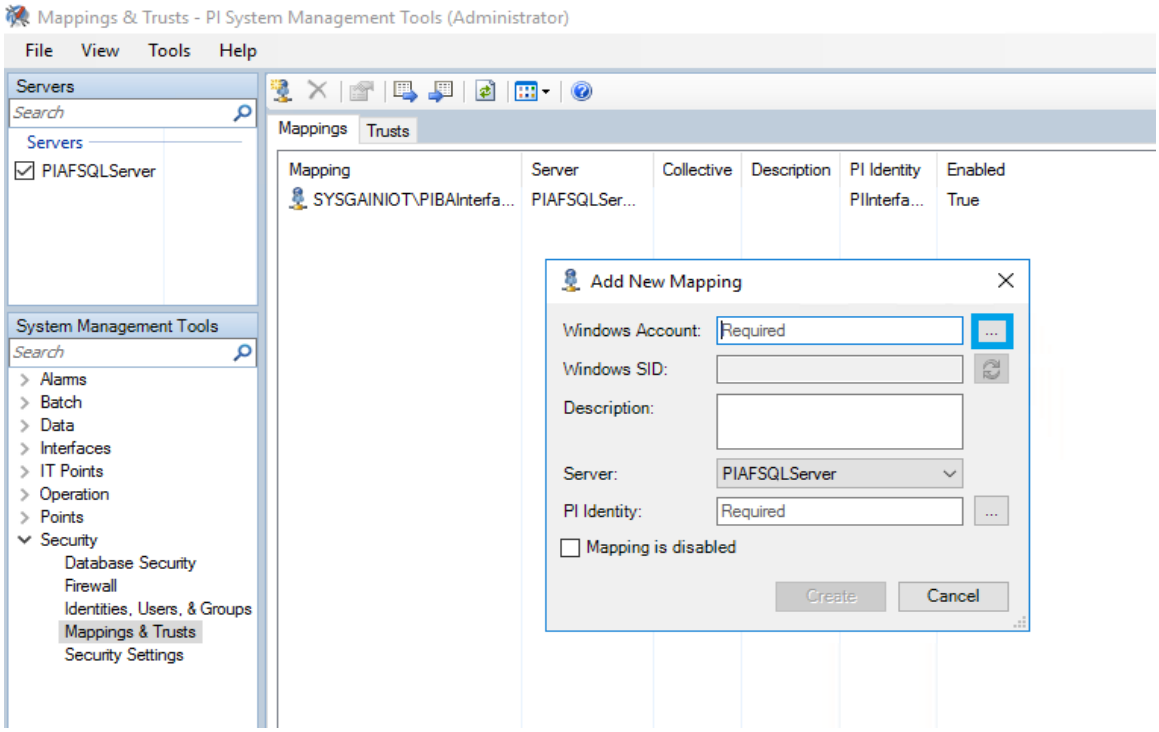
12. Click on **Create** to create a New Mapping for PIBAInterface.



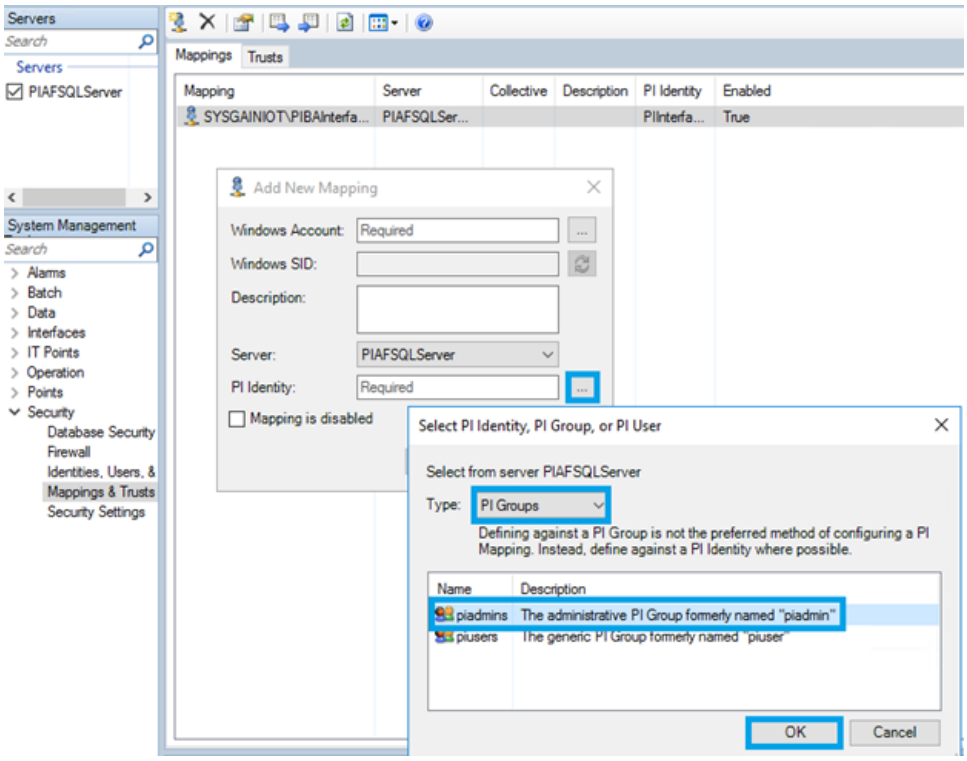
13. Click **OK** once the PIBAInterface mapping is created.



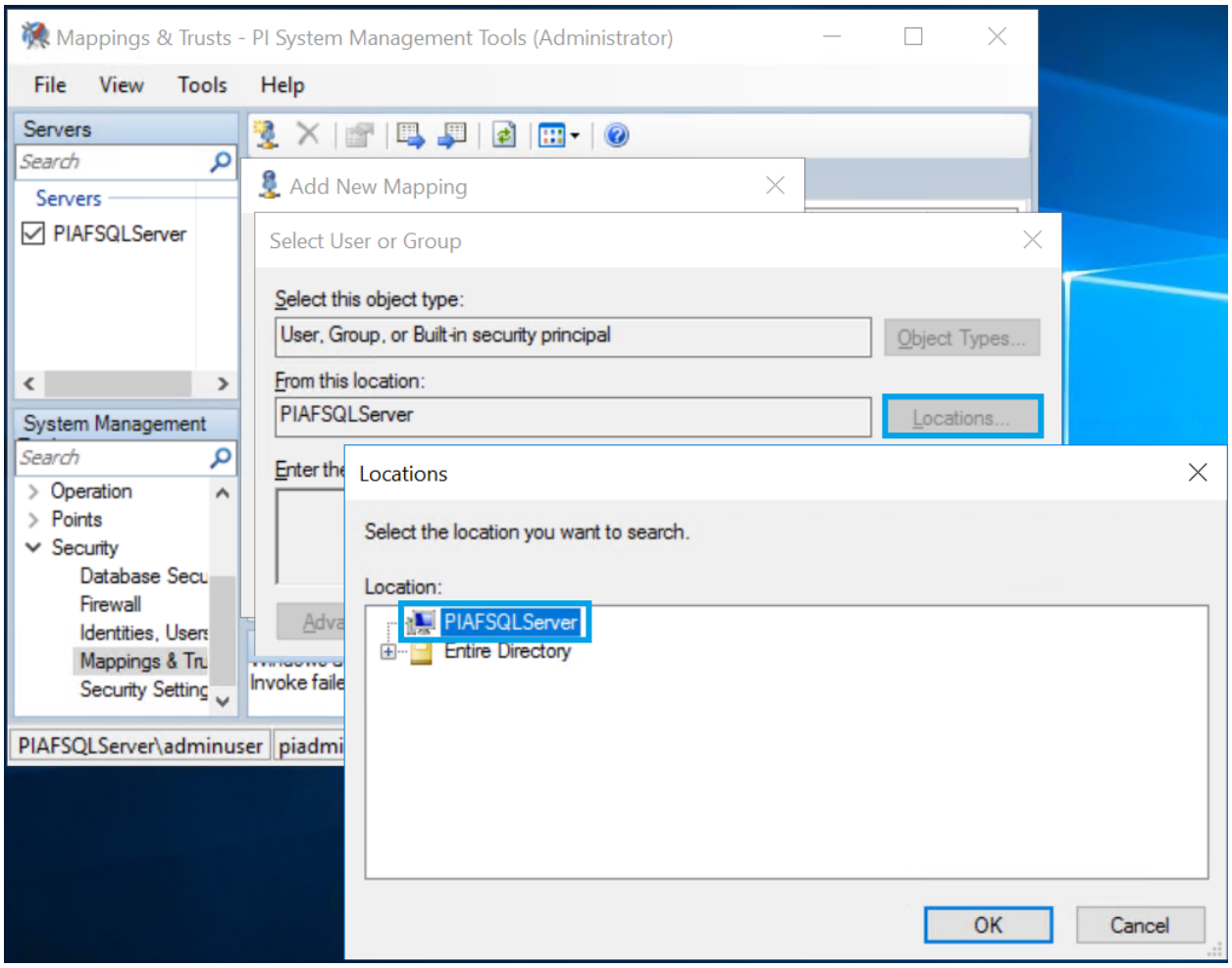
14. Navigate to **Security** > **Mapping & Trusts** to create a New Mapping.Click on the mappings above symbol to add new mapping.



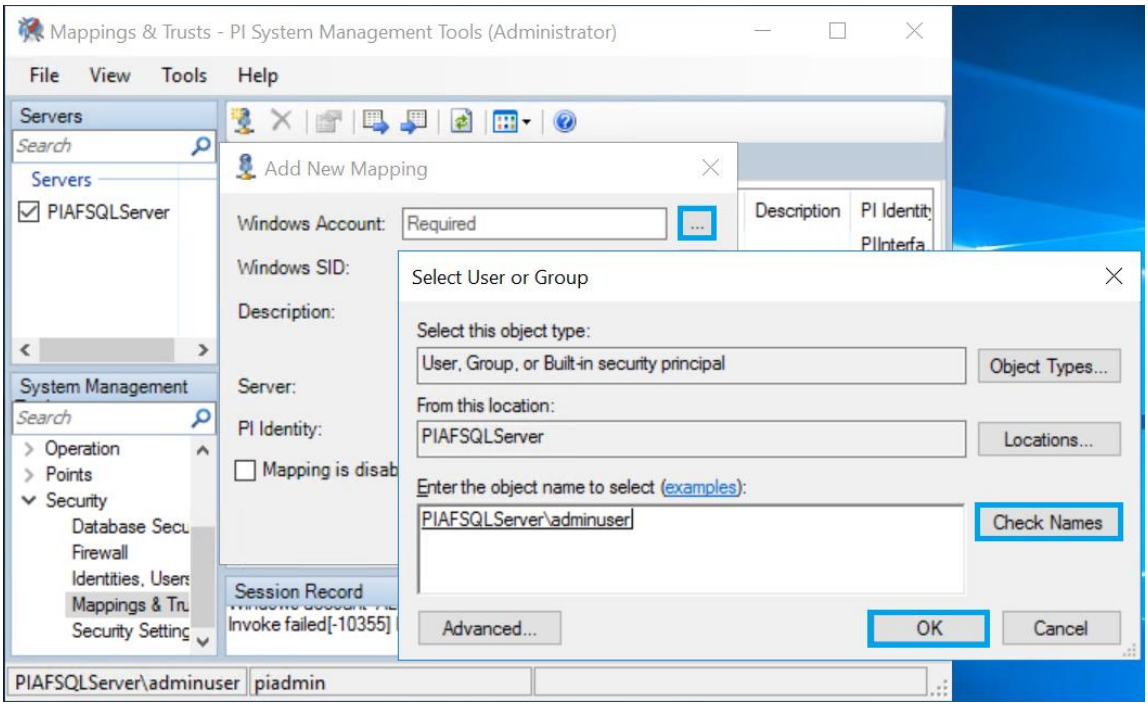
15. Browse the directory in **PI Identity** section, then select **PI groups** under the **Type** dropdown and Select **piadmins** to create PI Identity as **piadmins** click on **OK.**



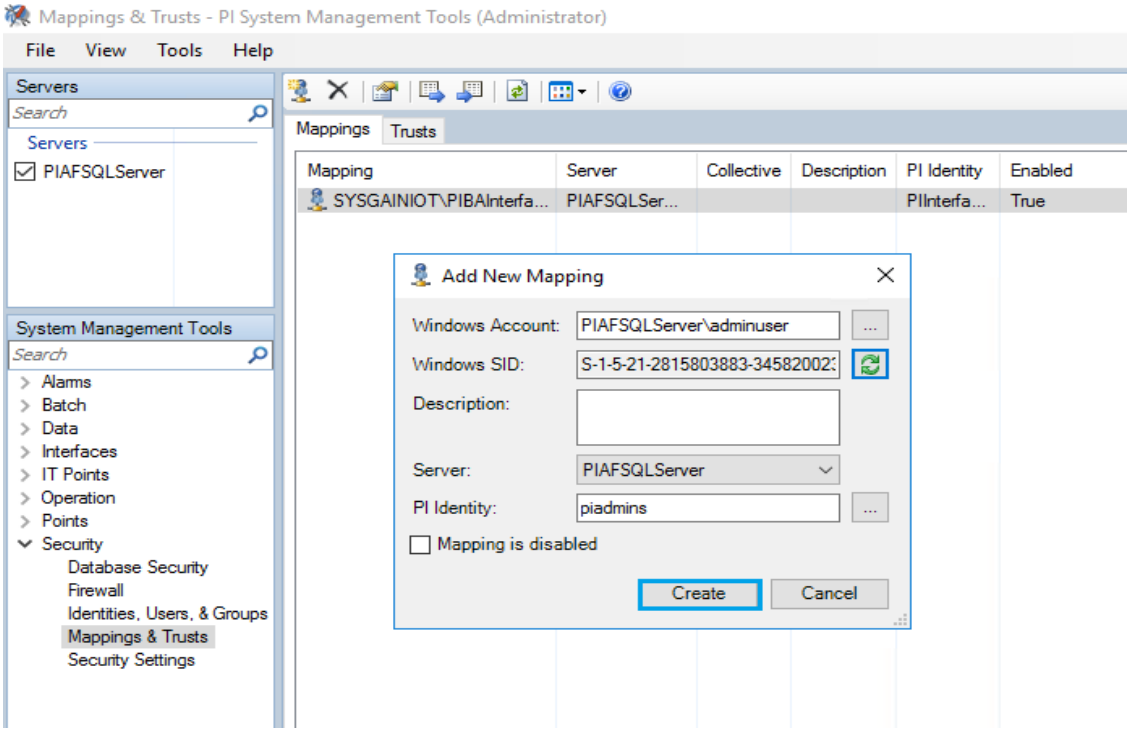
16. Click the dots next to **Windows Account**, then **Locations**, and select the **PIAFSQLServer**. Click on **OK**.



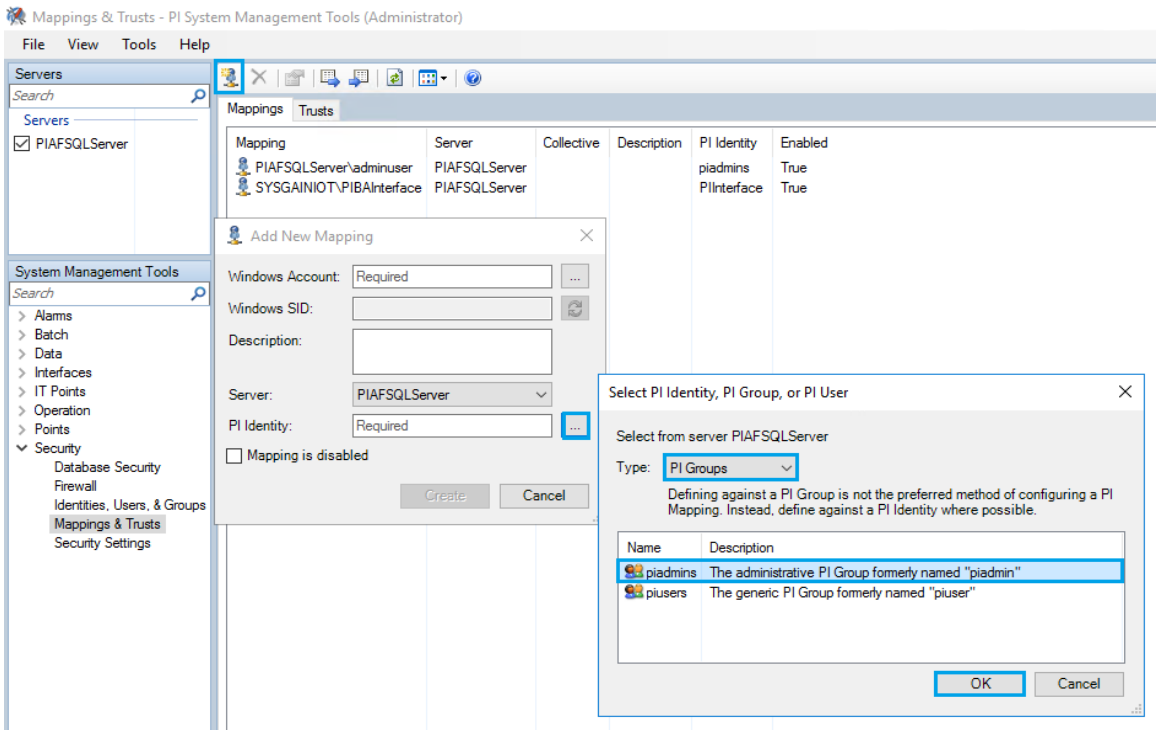
17. Under object name, type adminuser and click on **Check Names**, the following value **PIAFSQLServer\adminuser** will be populated automatically. Click on **OK.**



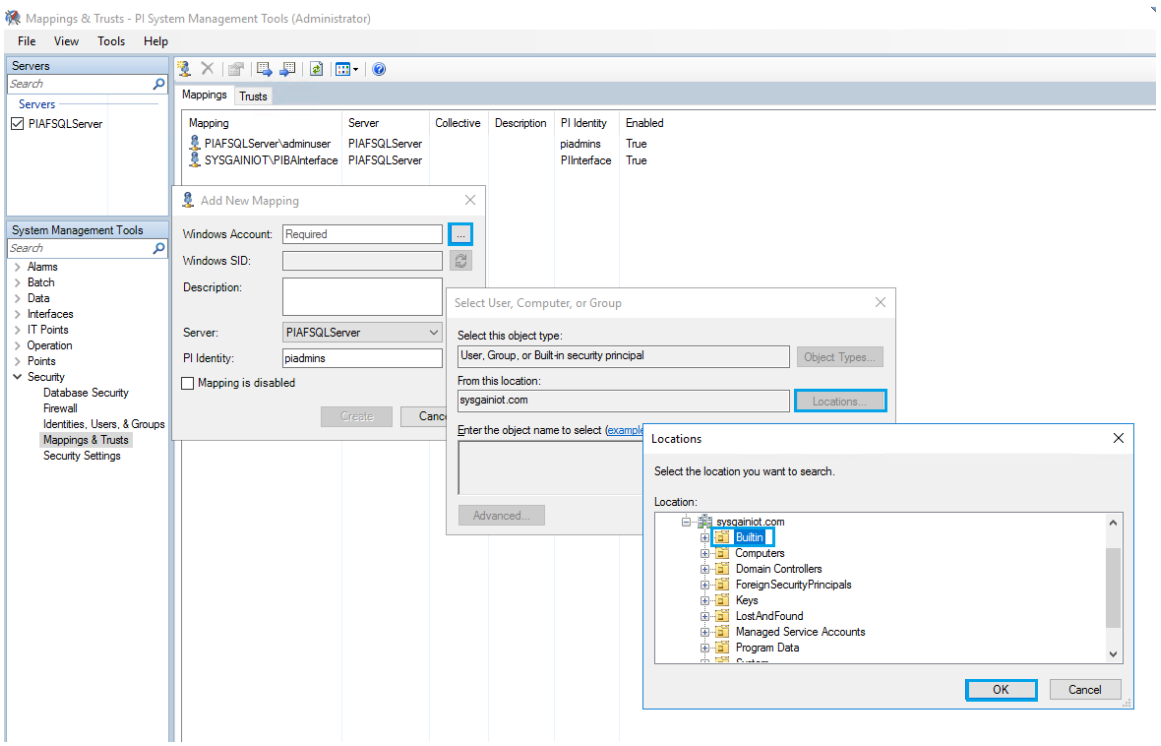
18. Click on **Create**



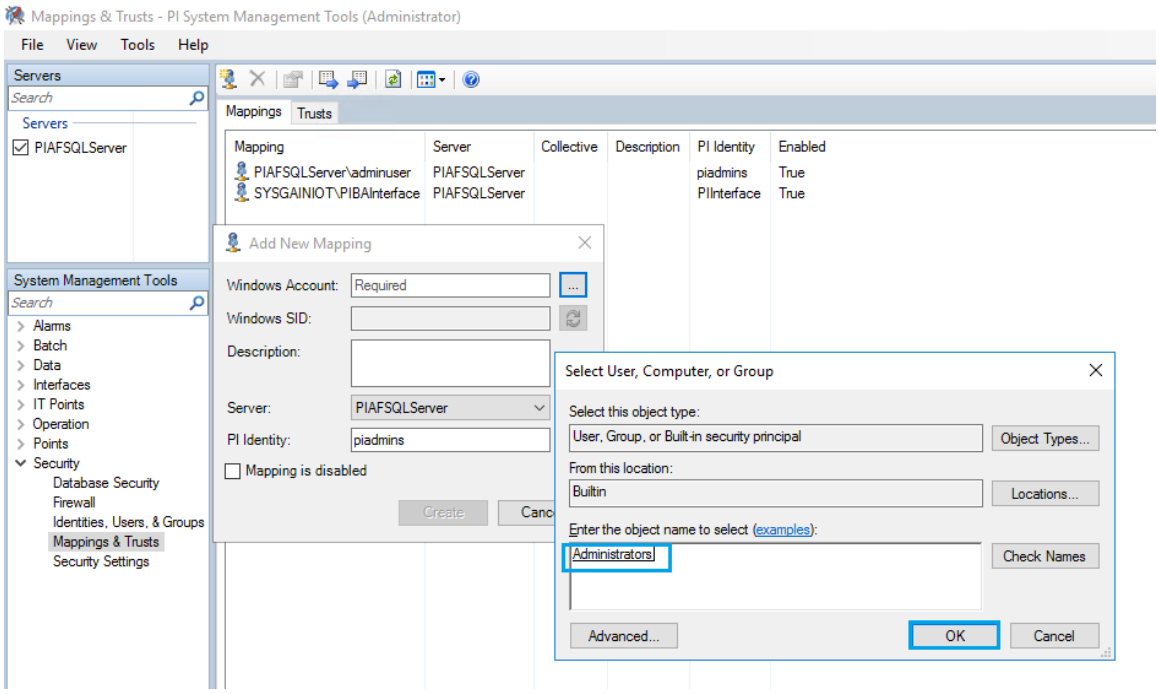
19. Create a new Mapping for **Administrator**.Click on the Mappings above symbol to add new mapping
20. Browse **PI Identity** end, select **Type as PI Groups** > Select **piadmins** > Click on **OK**.



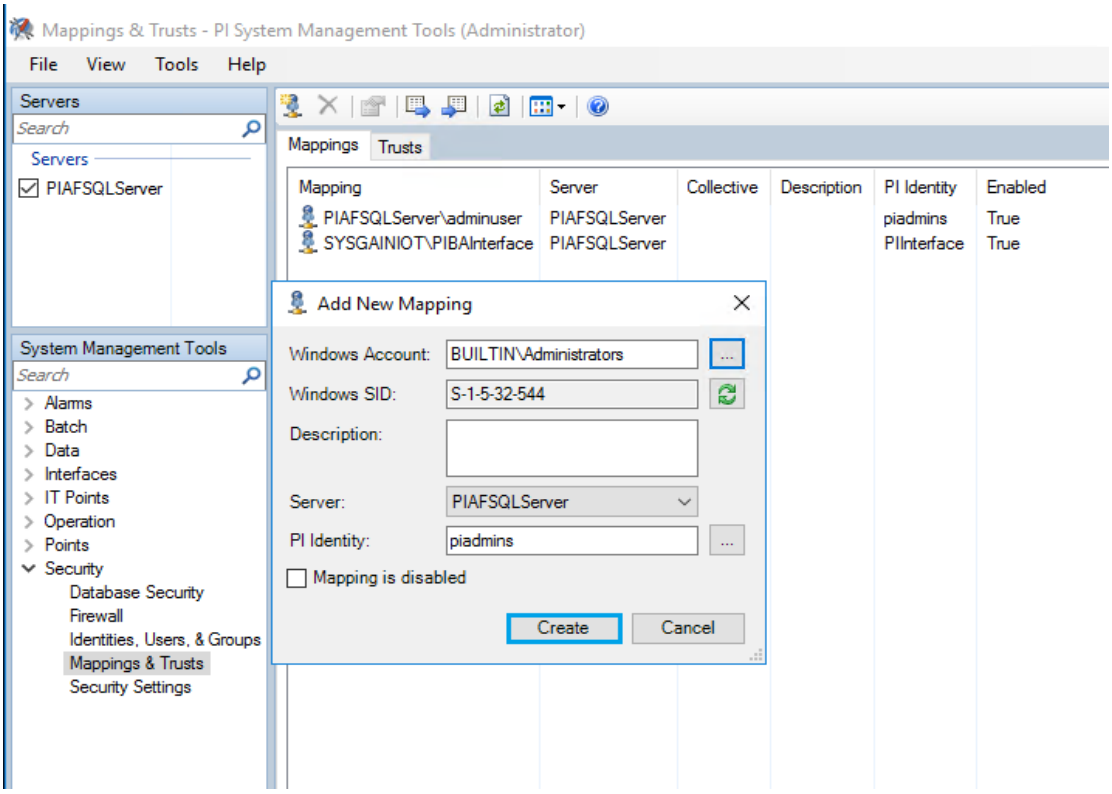
21. Click the Browse dots near **Windows Account** > Select **Locations** > click on **sysgainiot.com** > Select **Builtin** > Click **OK.**



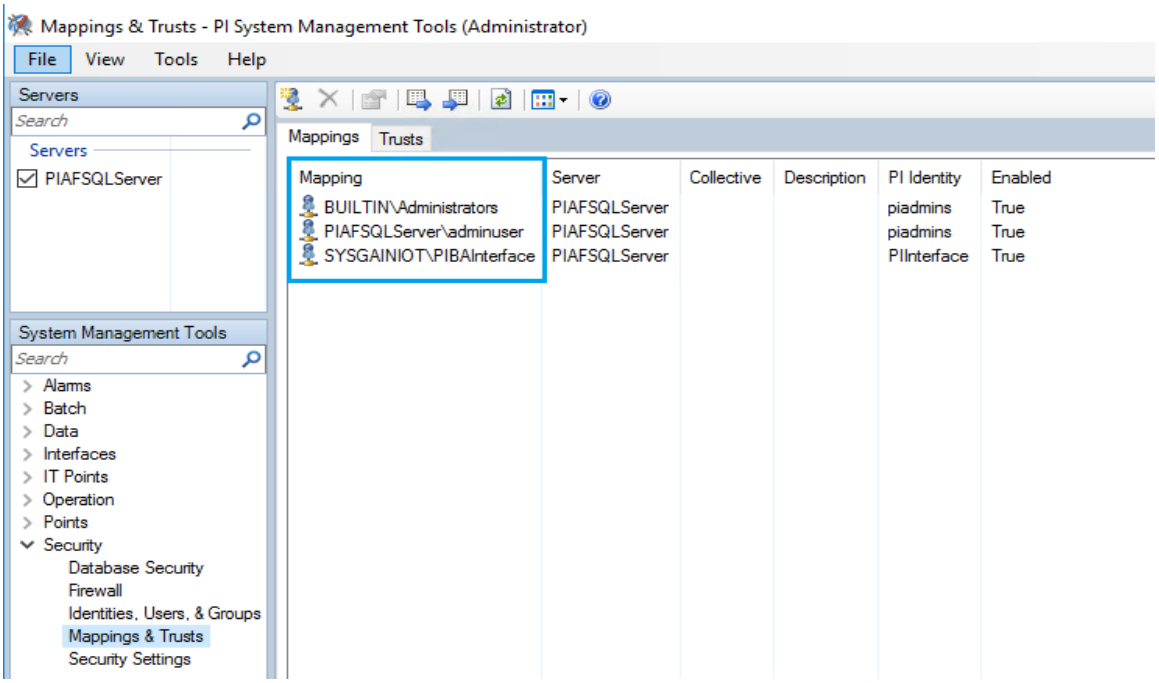
22. Enter the object name as **Administrators**, click on **Check Names** and click on **OK.**



23. Click on **Create**.

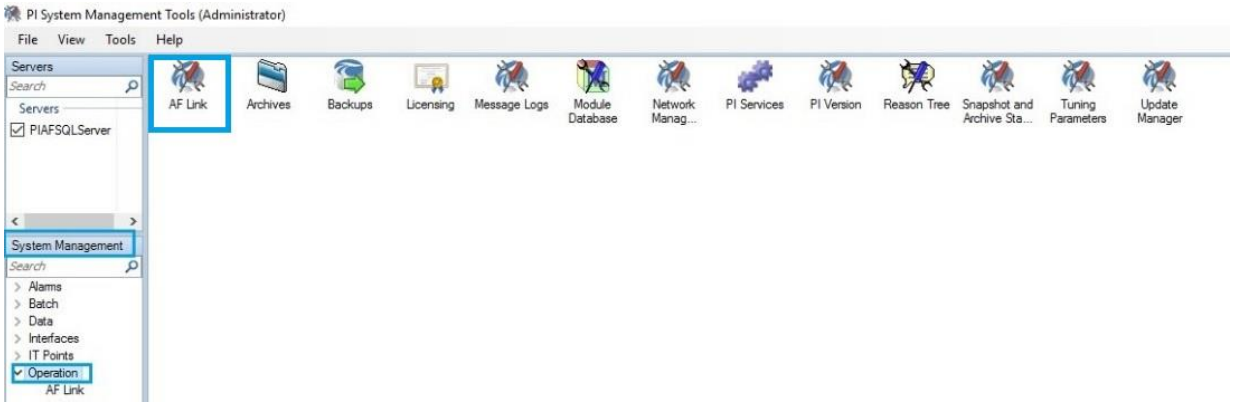


24. Verify the list of Mappings created.

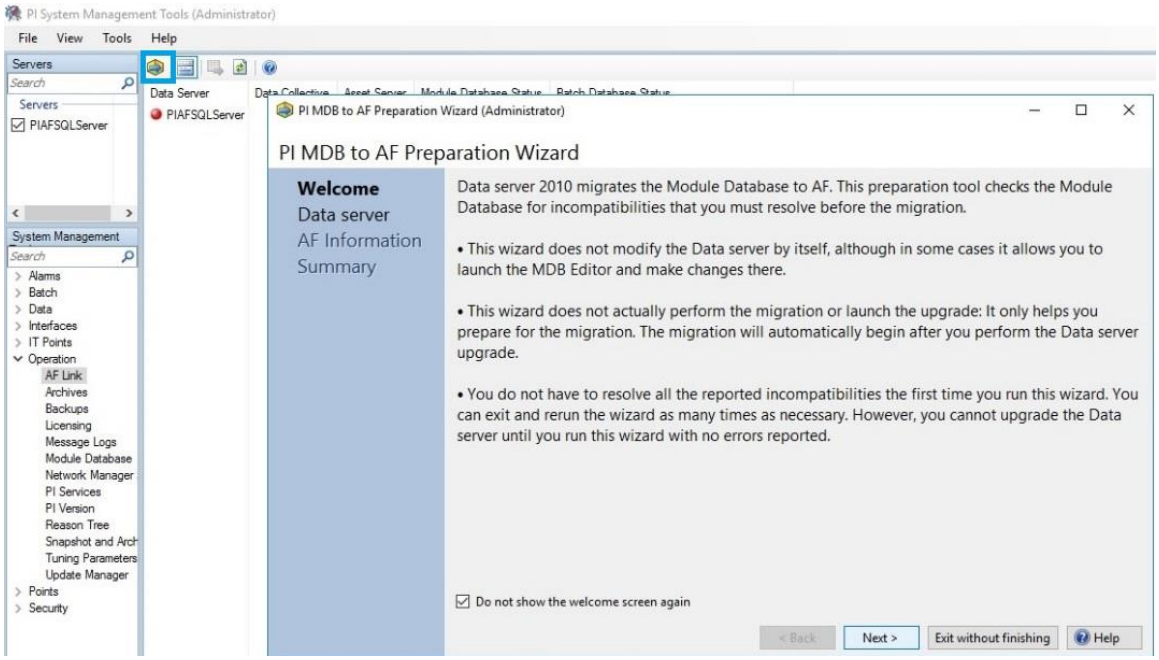


9.8. Prepare Data Server for Module Database(MDB) To Asset Framework(AF)

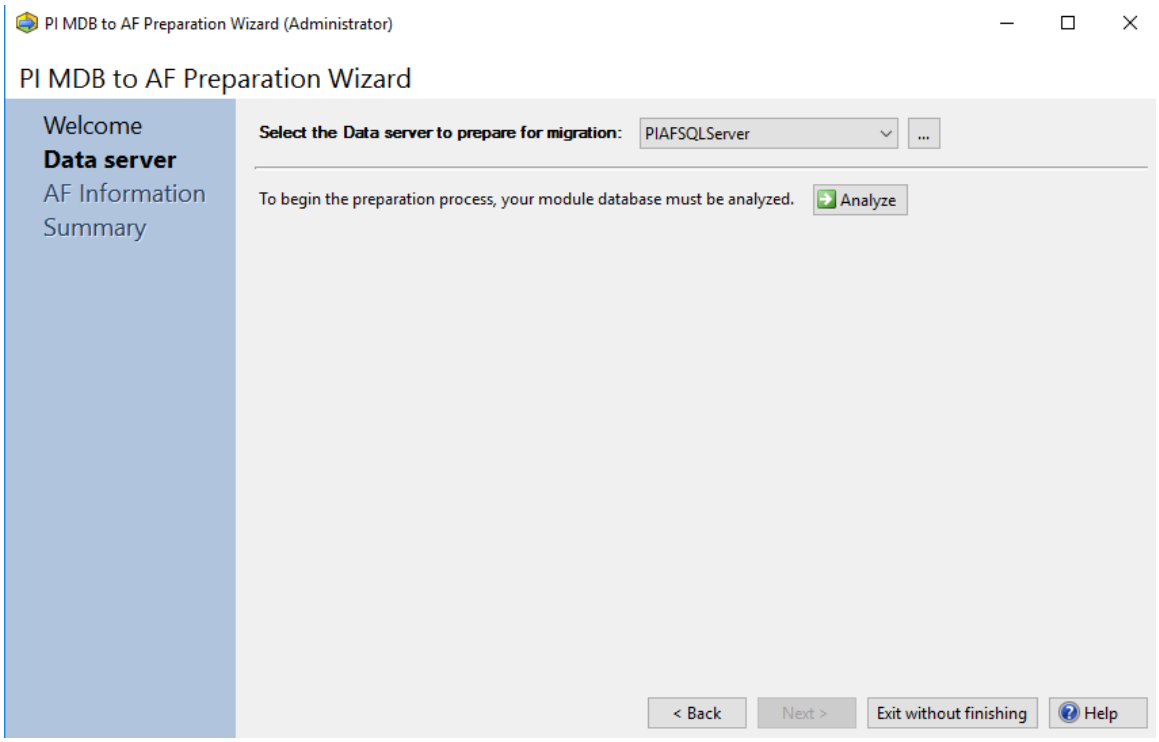
1. Navigate to **PI System Management Tools** > **Operation** > Click on **AF link**.

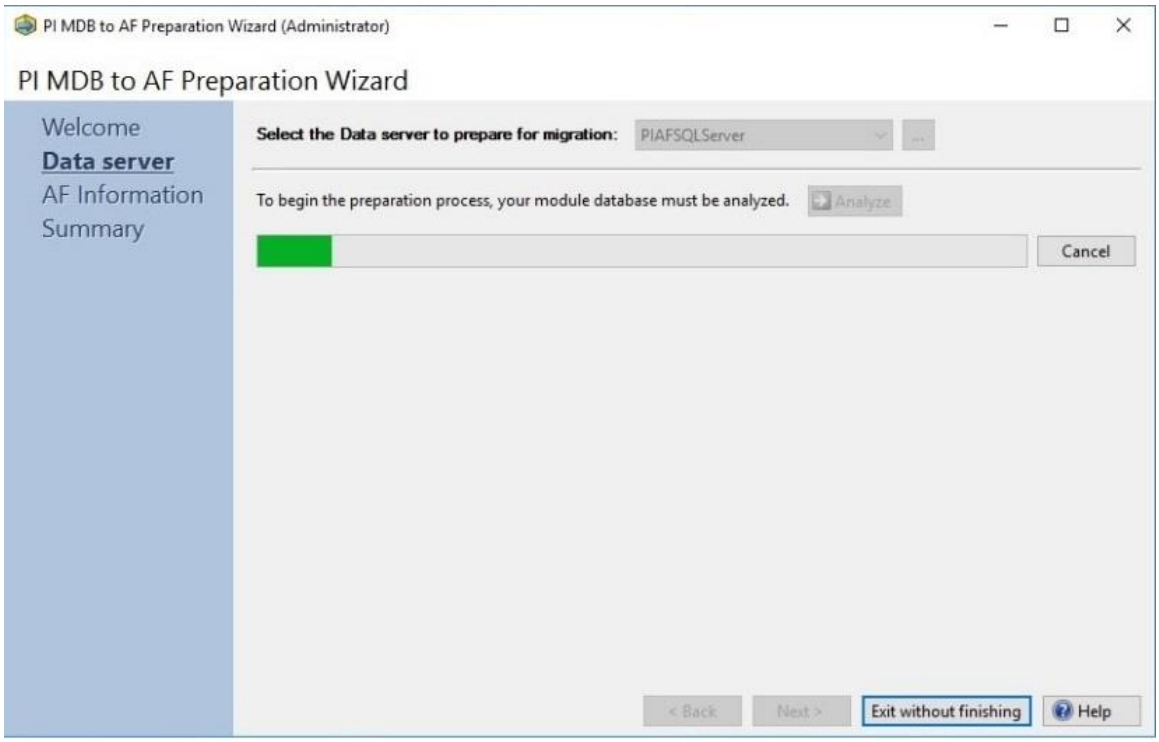


2. Click on **MDB to AF synchronization Wizard** (the symbol just below the **Help** tab). It will open the PI MDB to AF Preparation Wizard as shown below. Tick the do not show the welcome screen again checkbox ,Click on **Next**.

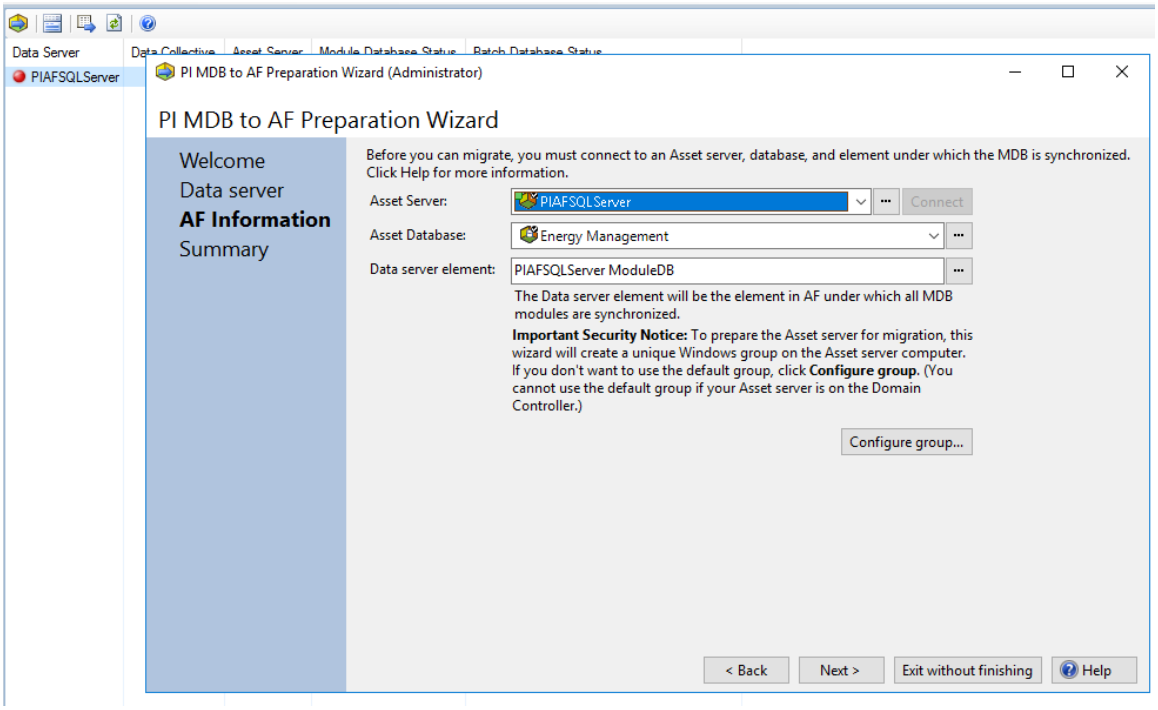


3. Click on **Analyze**, then click on **Next** and again click on **Next** once the process is complete.

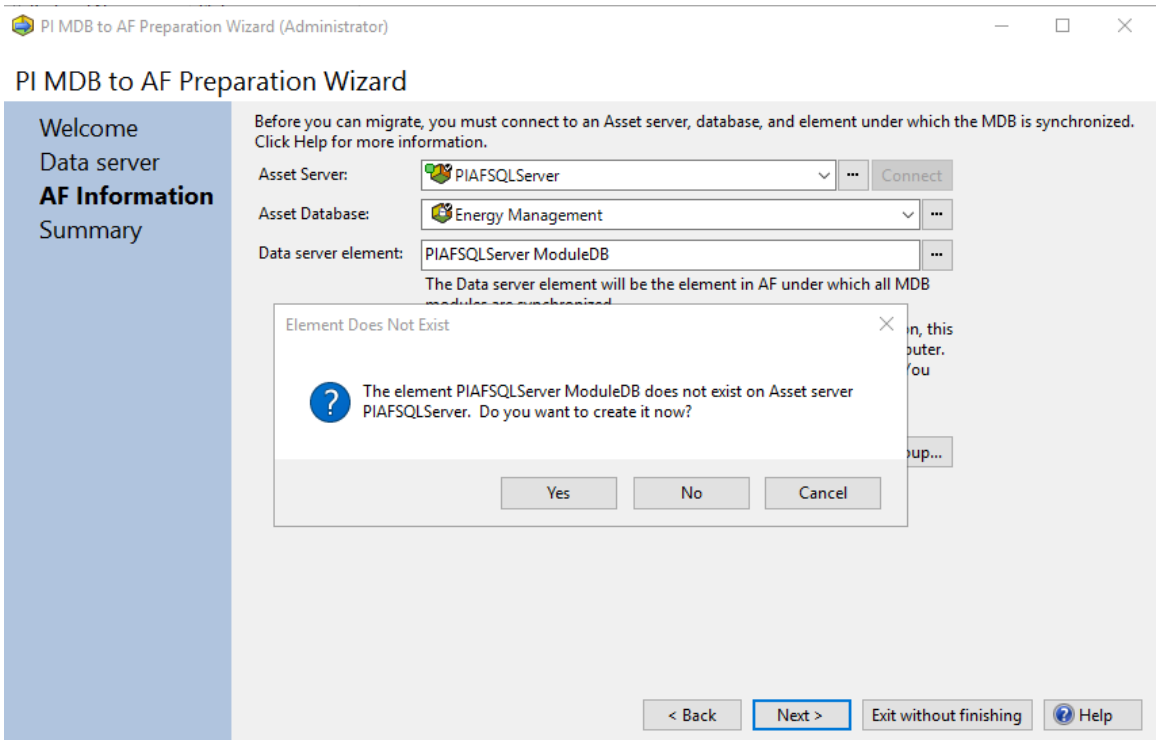




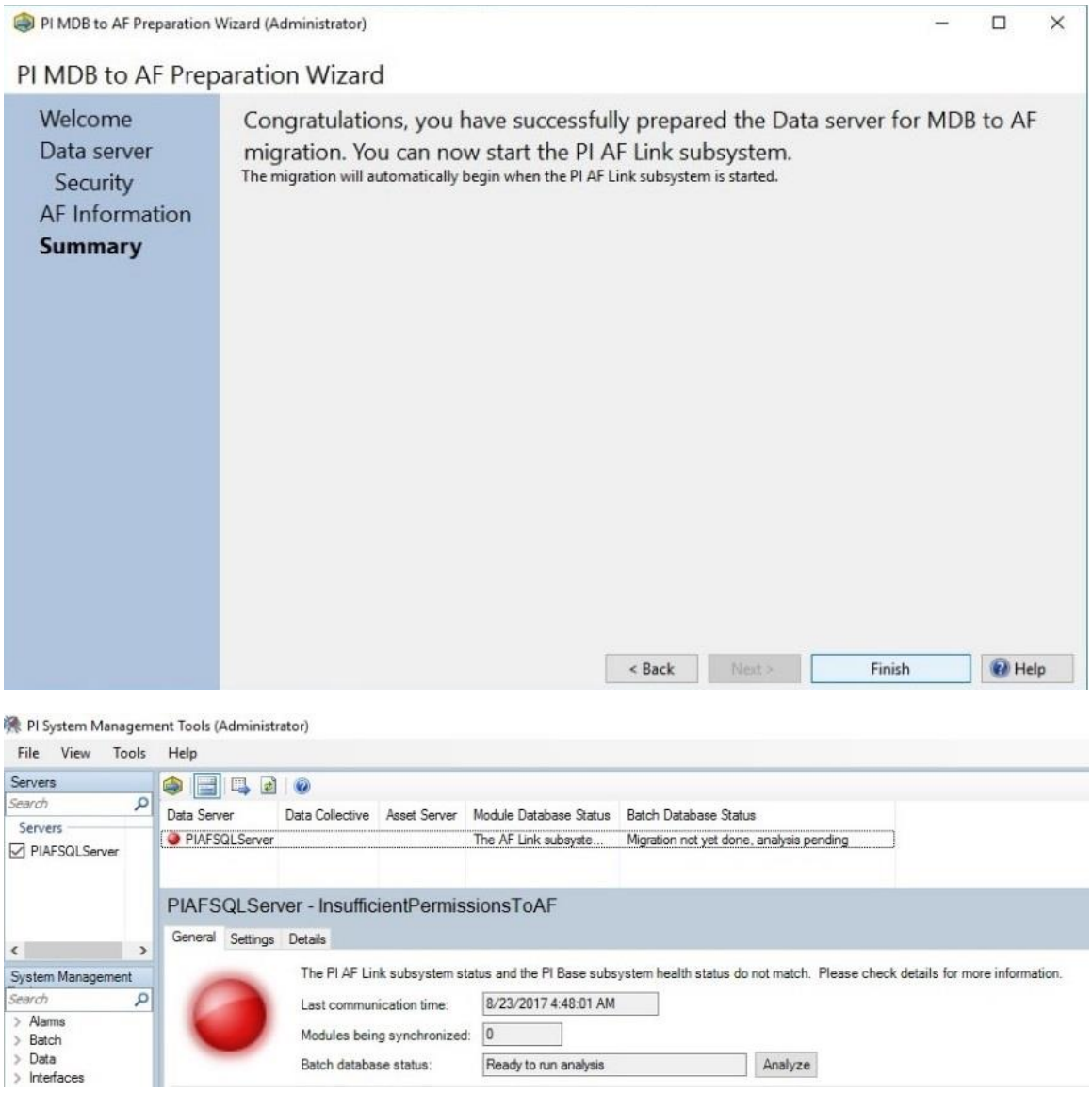
4. In AF Information, set the **Asset Server** as **PIAFSQLServer,** then click on **Connect.** Set **Asset Database** as **Energy Management**. Click on **Next**.



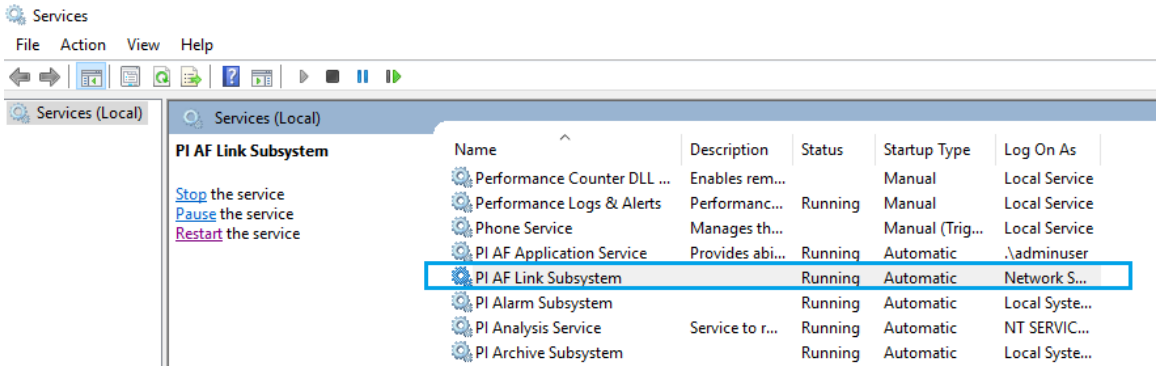
5. Click on **Yes** to create a PIAFSQLServer ModuleDB, then click on **Next**.



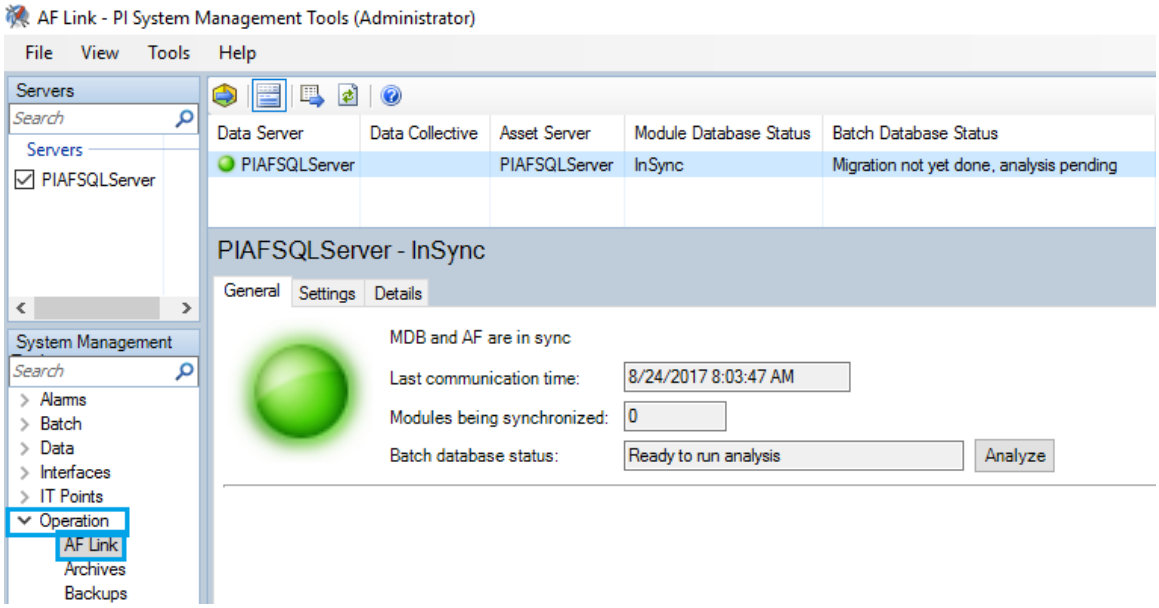
6. Click on **Finish**.



7. If you see the red circle on PIAFSQL Server, go to the **Services.msc** and restart the service **PI AF Link Subsystem**.

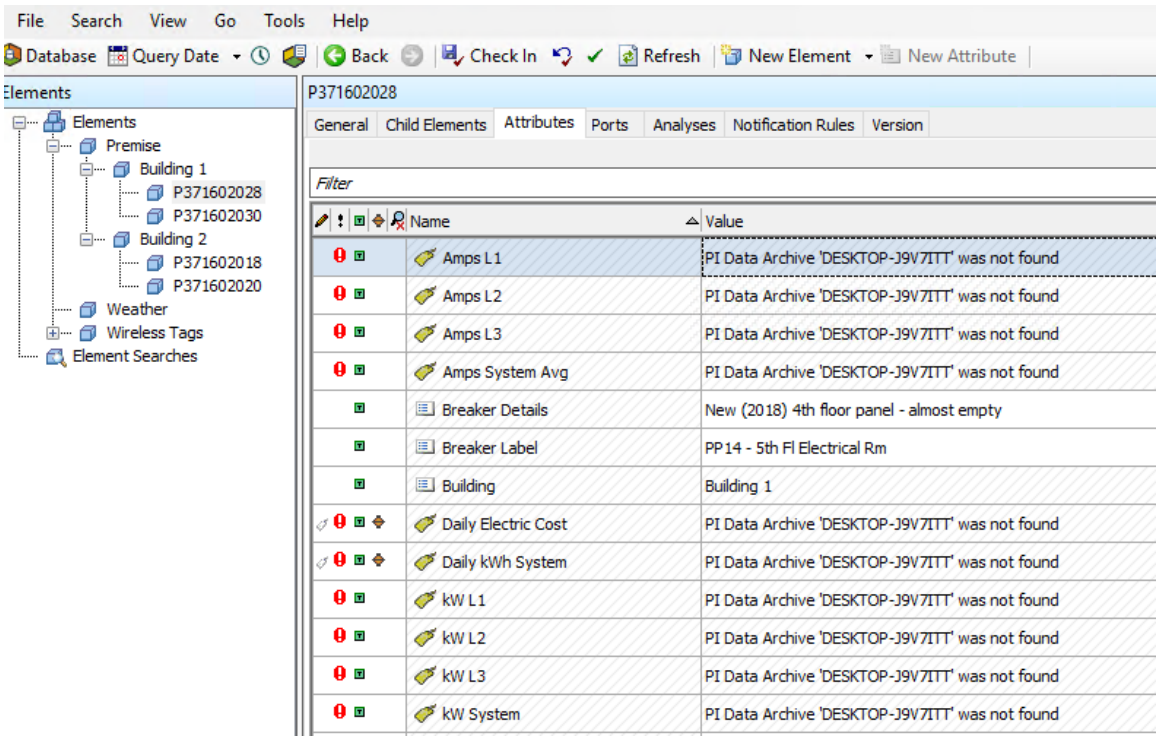


8. After restart, go to the **Operations** under system management and click on **AF Link.** You can see the PIAFSQL Server now has a green circle.



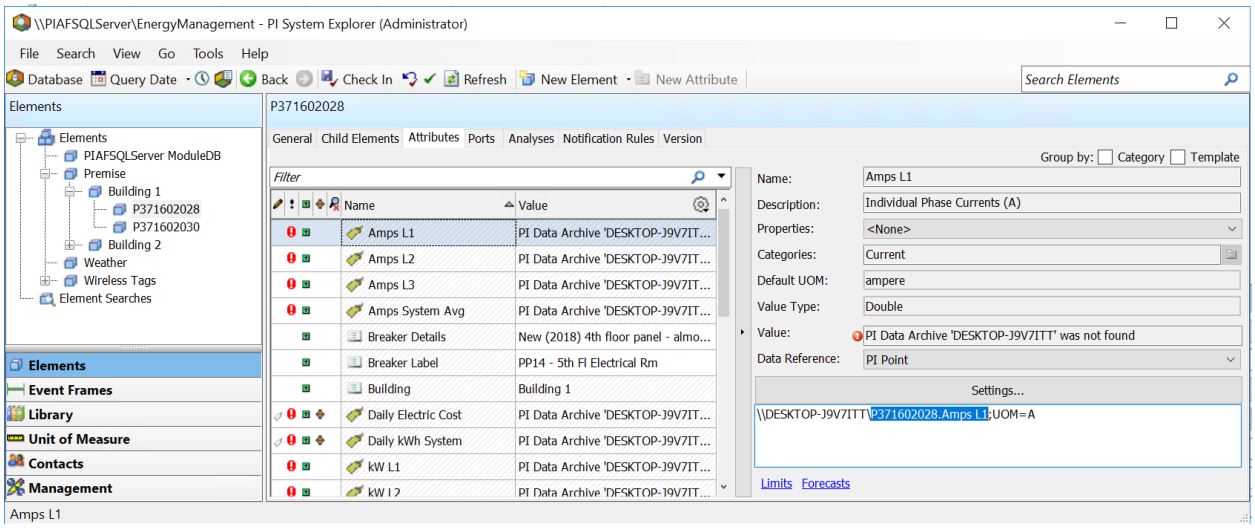
9.9. Update PI Points in PI System Explorer

1. Open **PI System Explorer** from the Start Menu in the PI System folder.
2. Navigate to **Elements** > **Premise** > Click on **Building1, Building2** > Click on **Attributes**. You will notice a red symbol next to some of the attributes. These Attributes must be updated.

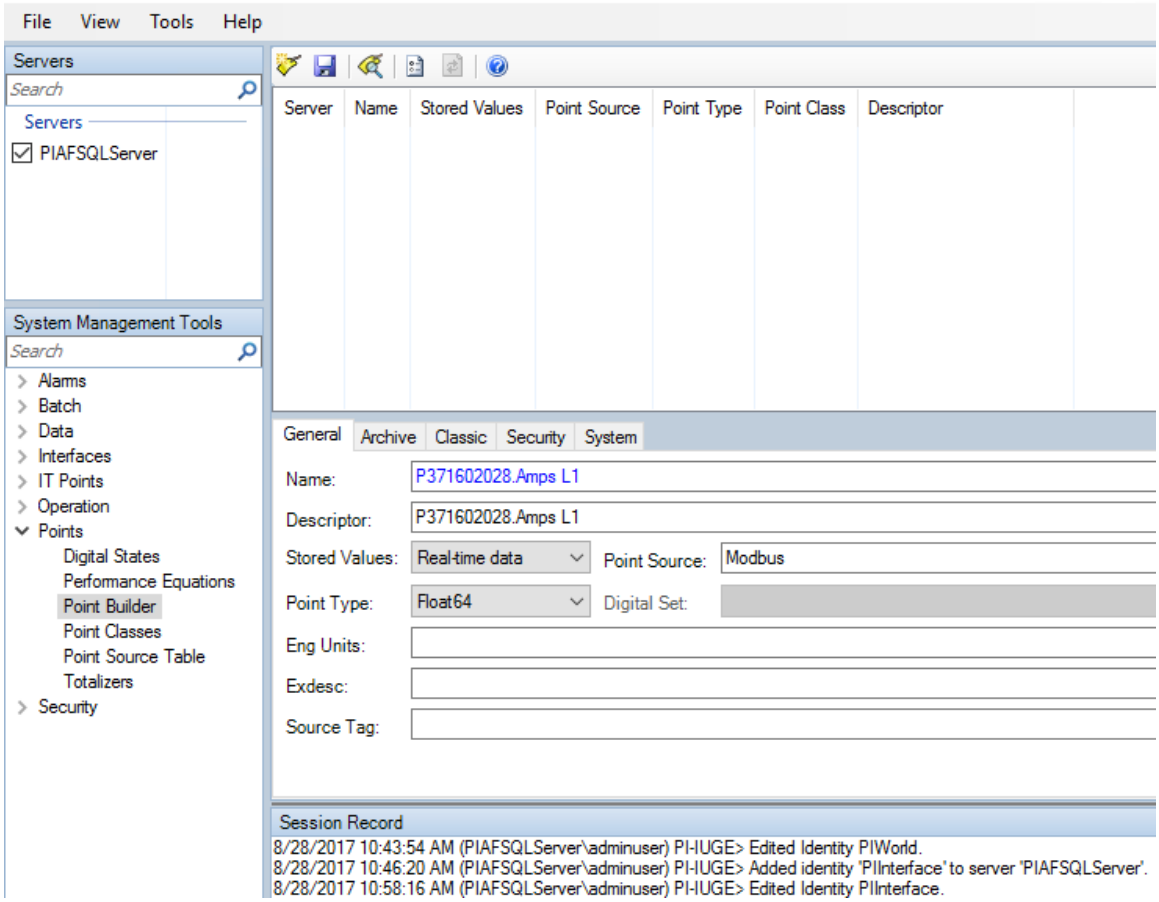


3. To update the attribute, click on a **Name.** Then, under Settings, copy the PI point as shown below.
   For example1, \\DESKTOP-J9V7ITT**P371602028.Amps L1**;UOM=A
   the highlighted part (the text between **"\"** and **";"**).

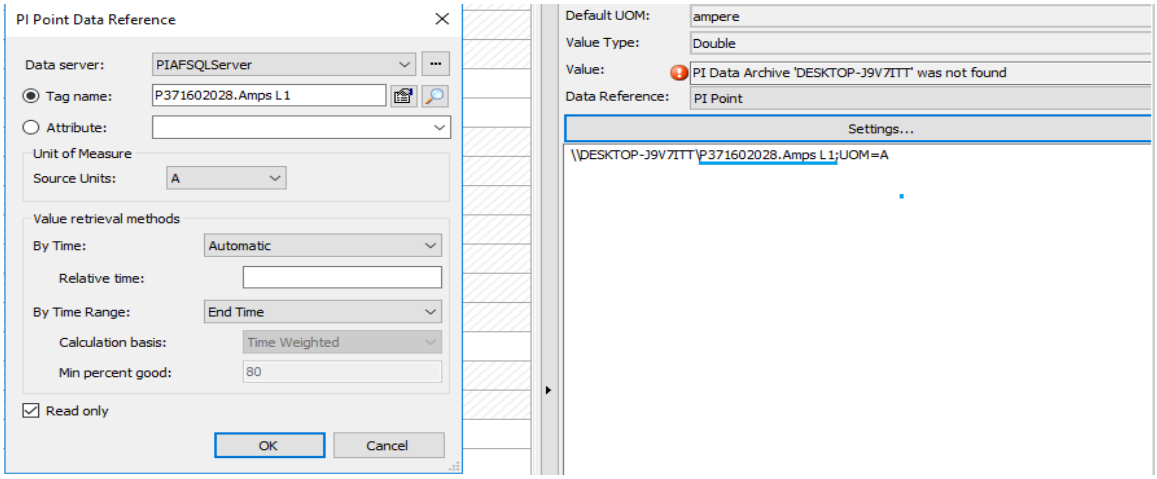
   For exxample2, \\DESKTOP-J9V7ITT**P371602028.Daily Electric Cost.60e6094f-e554-5e8f- 1742-54def61fbe81**
   In such cases copy full point after **" \ "**



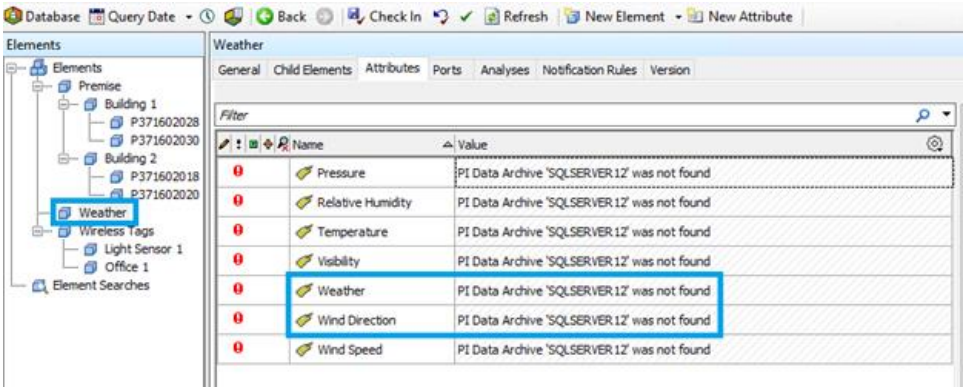
4. Open **PI System Management Tools** from the Start Menu in the PI System folder, then navigate to **Points** > **Point Builder.**
5. Paste the PI point content copied from PI explorer in the **Name** and **Descriptor** fields**.**
   Enter **Point Source** as **"Modbus"**, then **Point type** as **Float 64.**
6. Click on **Save.**

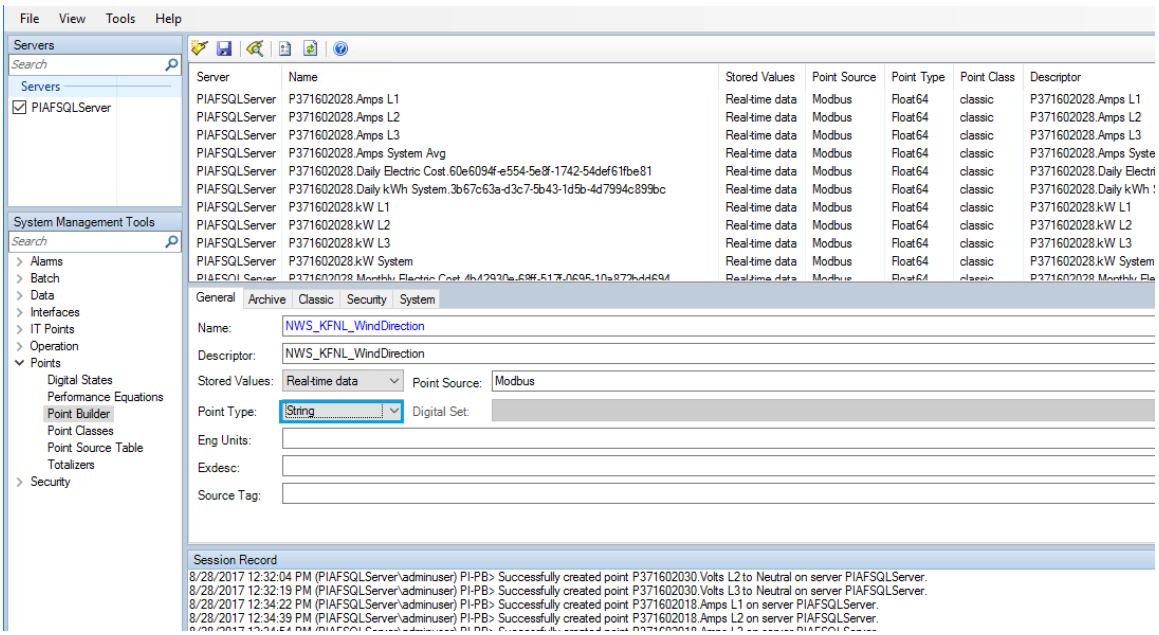


7. Go to **PI System Explorer,** click on **Settings,** and you will see the following dialog box. Under "Data Server", select the **PIAFSQLServer** and click on **OK.**



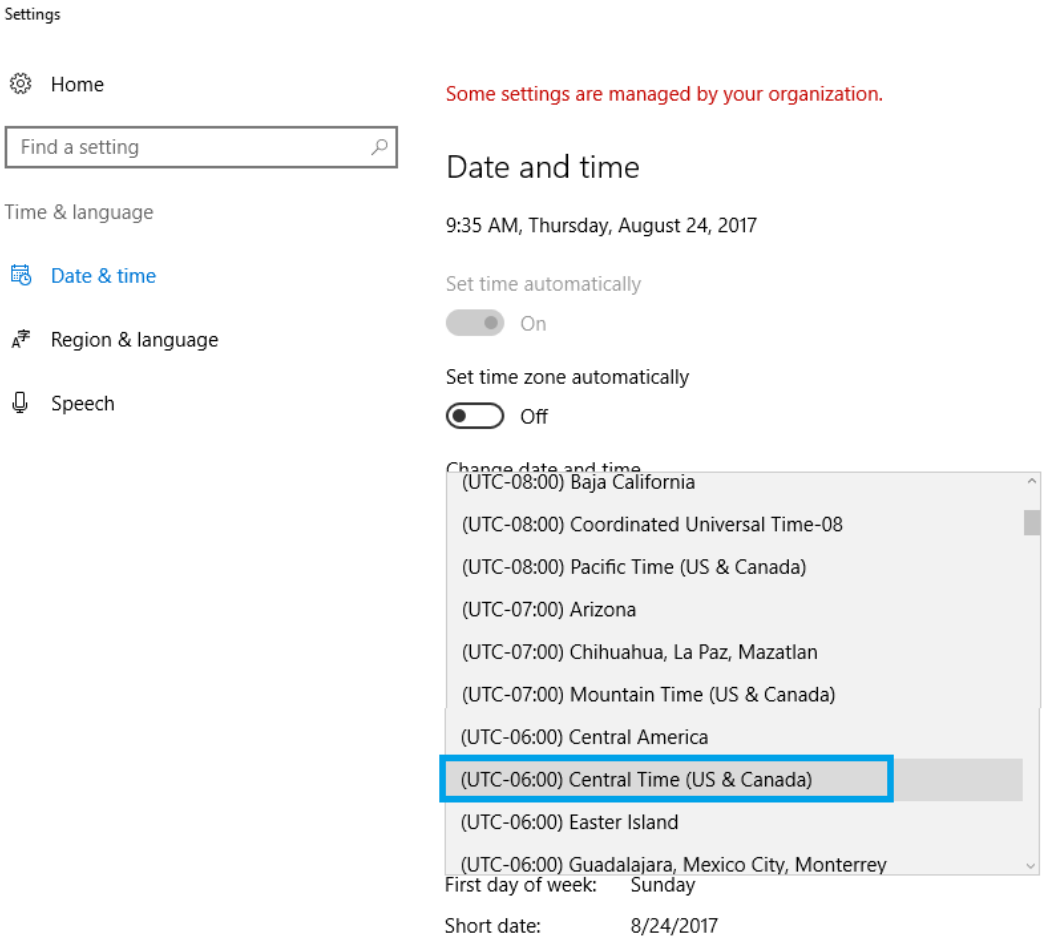
8. Update for all the Elements under the Premise, Weather, and Wireless tags.
9. under **Weather** for **Wind Direction** and **Weather,** the **Point Type** should be updated as **"String"** as shown below.



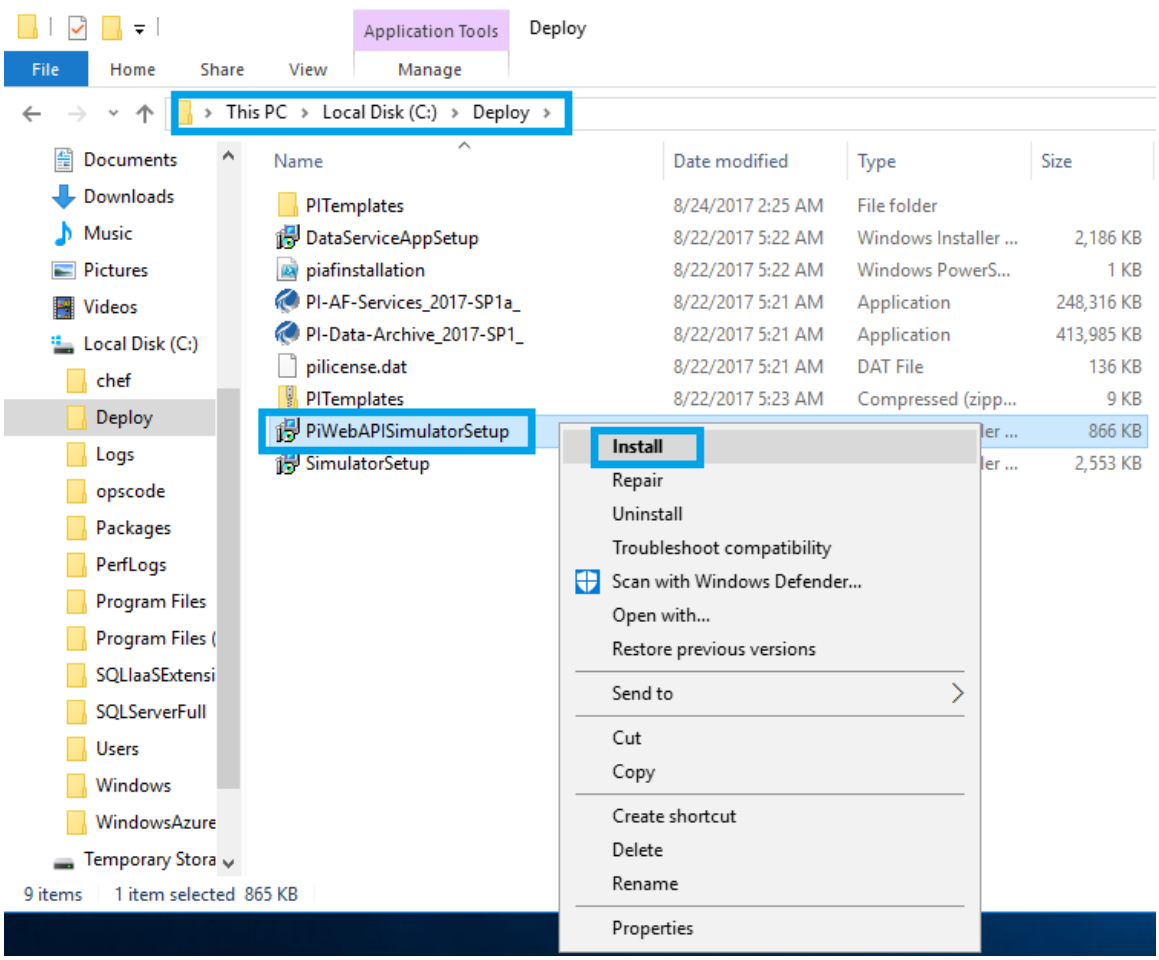


9.10. Install and Run The Piweb Simulator Setup

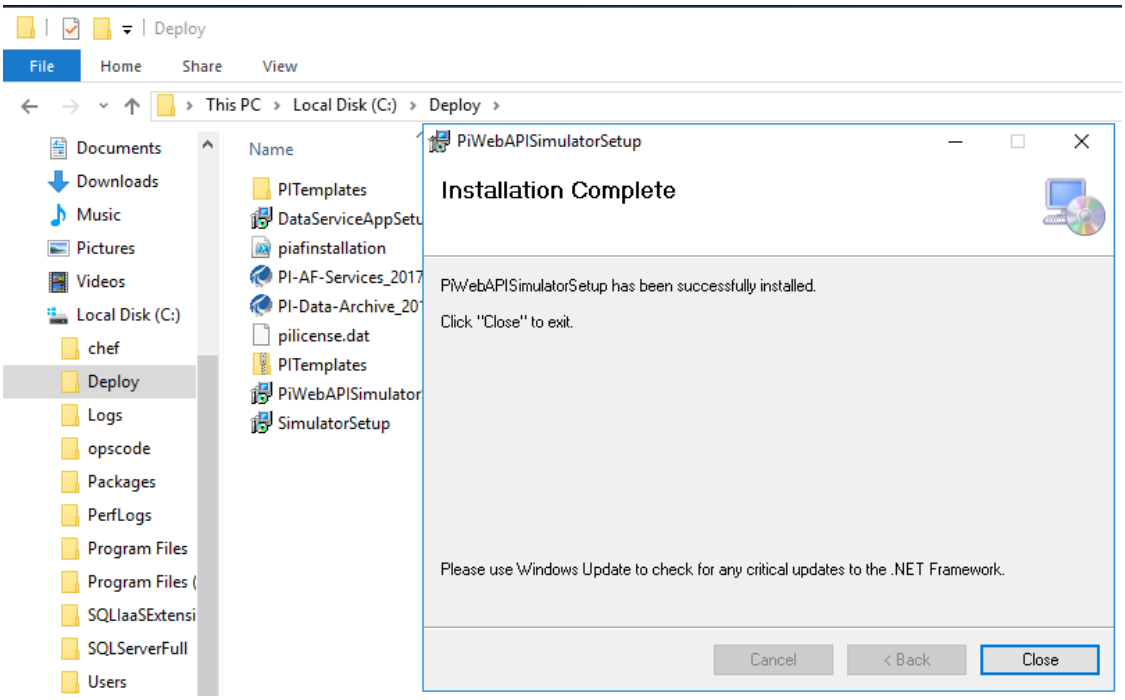
1. Change the time stamp to **(UTC-06:00) Central Time (US&Canada)**



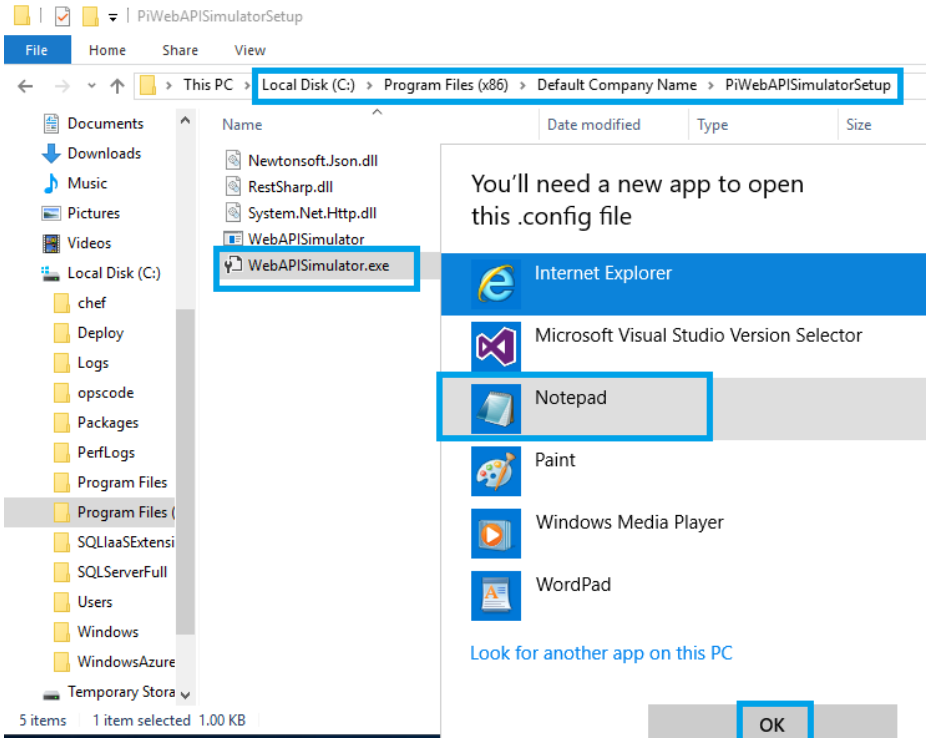
2. Navigate to the **Local Disk (C:)** > **Deploy** > **PIWebAPISimulatorSetup** and right-click to **Install.**



3. Click on **Close** after the installation complete.



4. Navigate to the **Local Disk (C:) > Program Files(X86) > Default Company Name > PiwebAPISimulatorSetup**. Under that select the **WebAPISimulator.Exe** and open with notepad, click on **OK**.



5. Update the Values under Appsettings section as below.

Replace the **Username** value with your domain name **without .com** \ PIAFSQLServer username

Replace the **Password** value with your PIAFSQLServer VM password

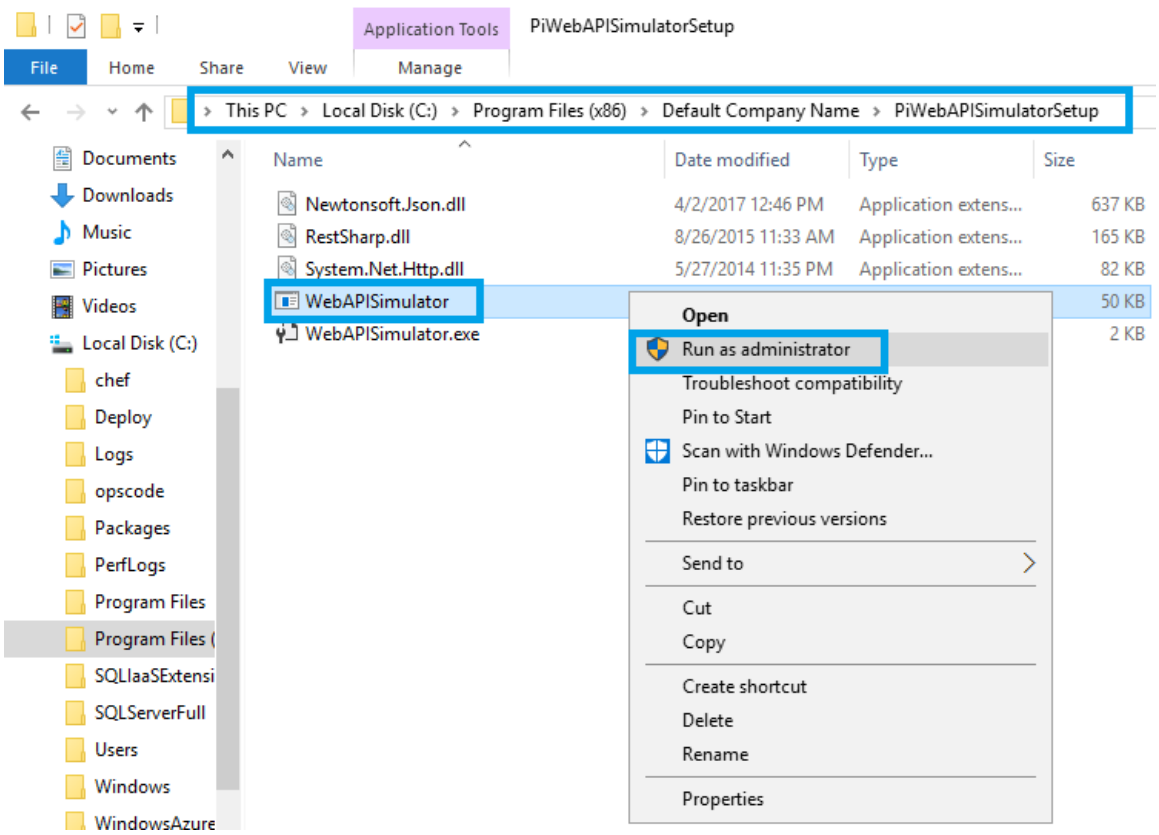
Replace the **BaseURL** value with the URL which you got during **9.3. PI web API utility** step 7 end we submit one url take that URL.

Remaining values replace same as below screenshot.

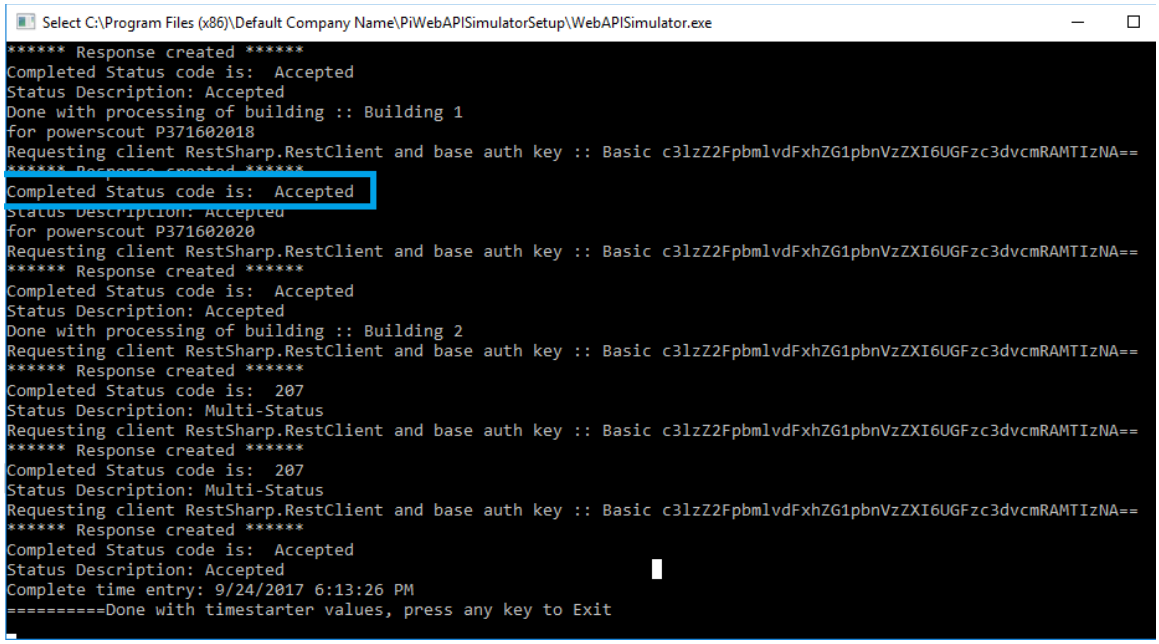
```
<add key="UserName" value="sysgainiot\adminuser" />
<add key="Password" value="Password@1234"/>
<add key="BaseURL" value="https://piafsqlserver.sysgainiot.com/piwebapi/"/>
<add key="DatabaseName" value="EnergyManagement"/>
<add key="PowerGridElementName" value="Premise"/>
<add key="WeatherElementName" value="Weather"/>
<add key="SensorElementName" value="Wireless Tags"/>
<add key="TimeStarter" value="0"/>
```

After updating all the values, click on **Save**.

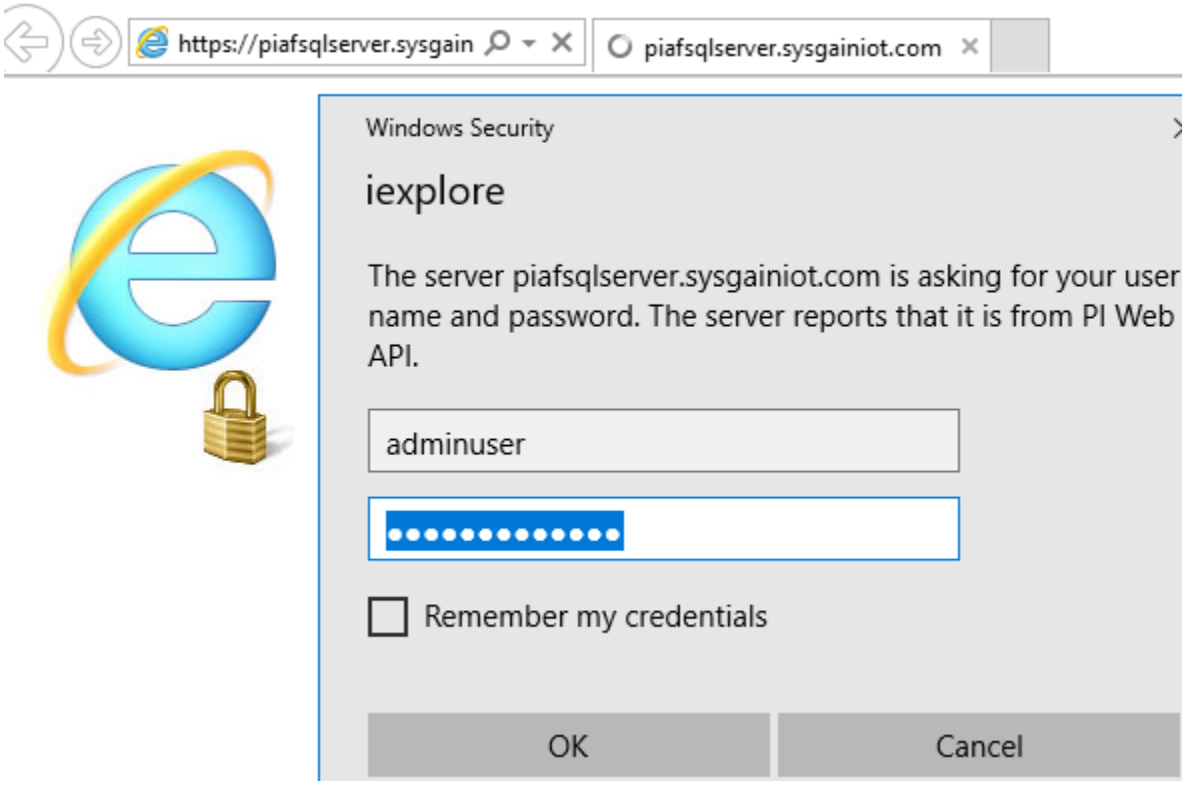
6. Navigate to **Local Disk (C:)** > **Program Files(X86)** > **Default Company Name** > **PiwebAPISimulatorSetup**. Select the **WebAPISimulator,** right click to **Run as Administrator**.



7. **Completed status code** should show as **Accepted**, which confirms that PIWebAPI Simulator is working.

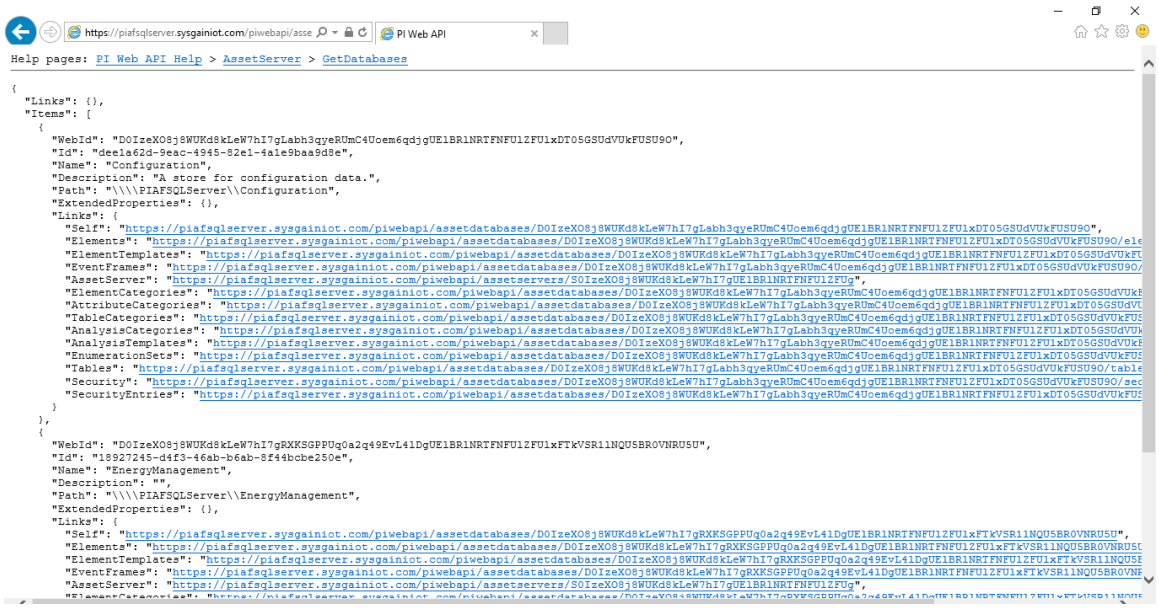


8. Paste the URL https://piafsqlserver.sysgainiot.com/piwebapi/ in **Internet Explorer** to view the Data servers URLS.It will show a popup box like below.Enter PIAFSQLServer credentials to login.



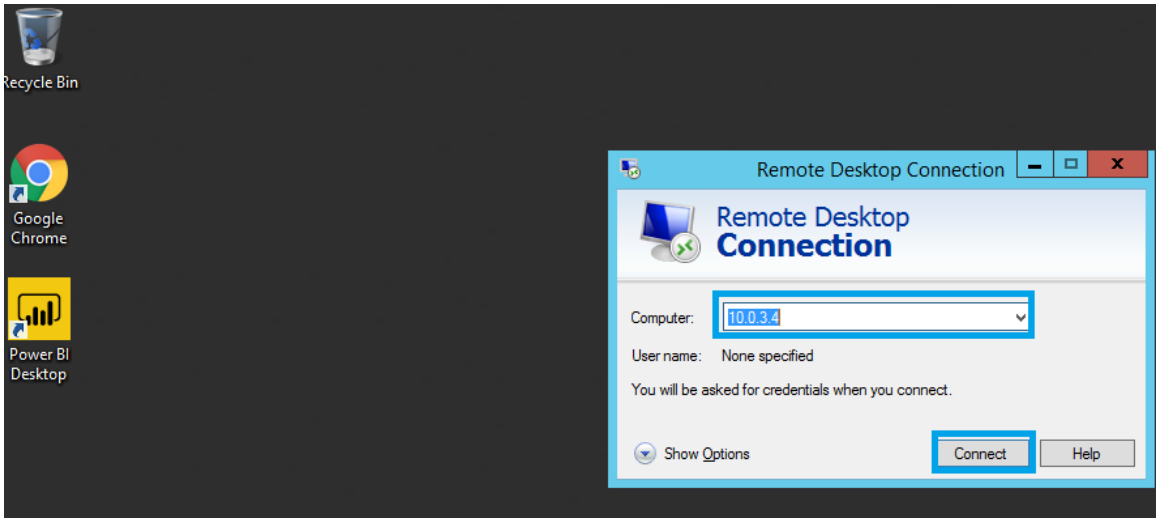
Once you login you can view the asset serversurls in internet explorer

9. To view the **Asset server** links, copy the Asset server link paste it in browser you can the Asset server links, click on databases to view the configuration and energy management items



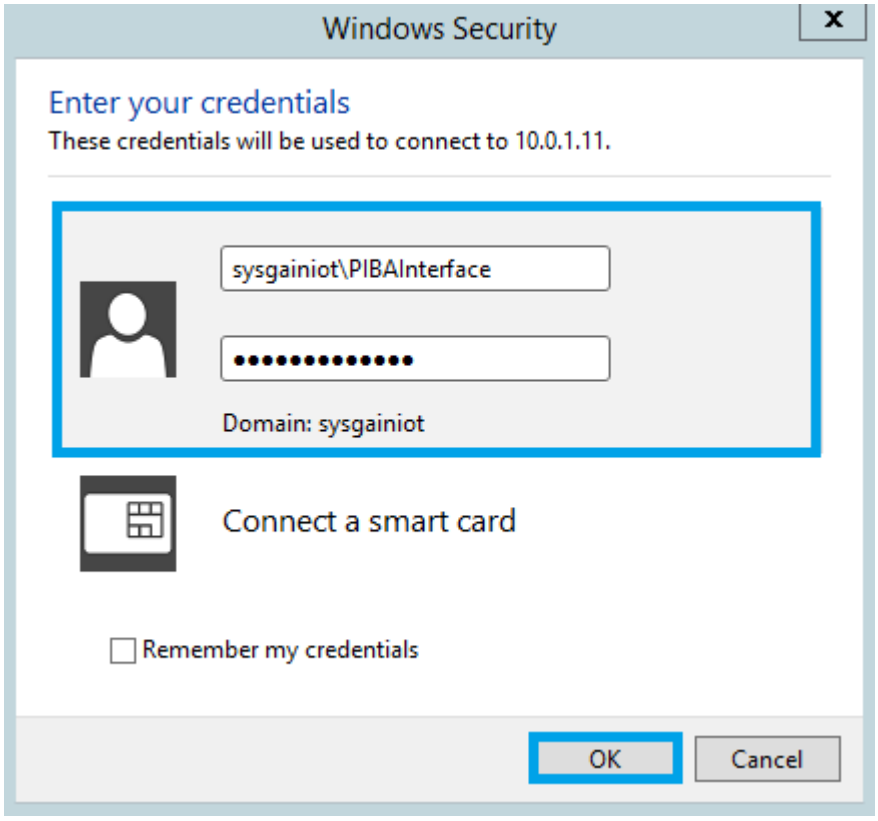
10. Installation of PI BA Integrator

1. From Bastion server, connect to the Remote server PIBA VMserver with details provided in output section name as **PIBASERVERIPADDRESS**

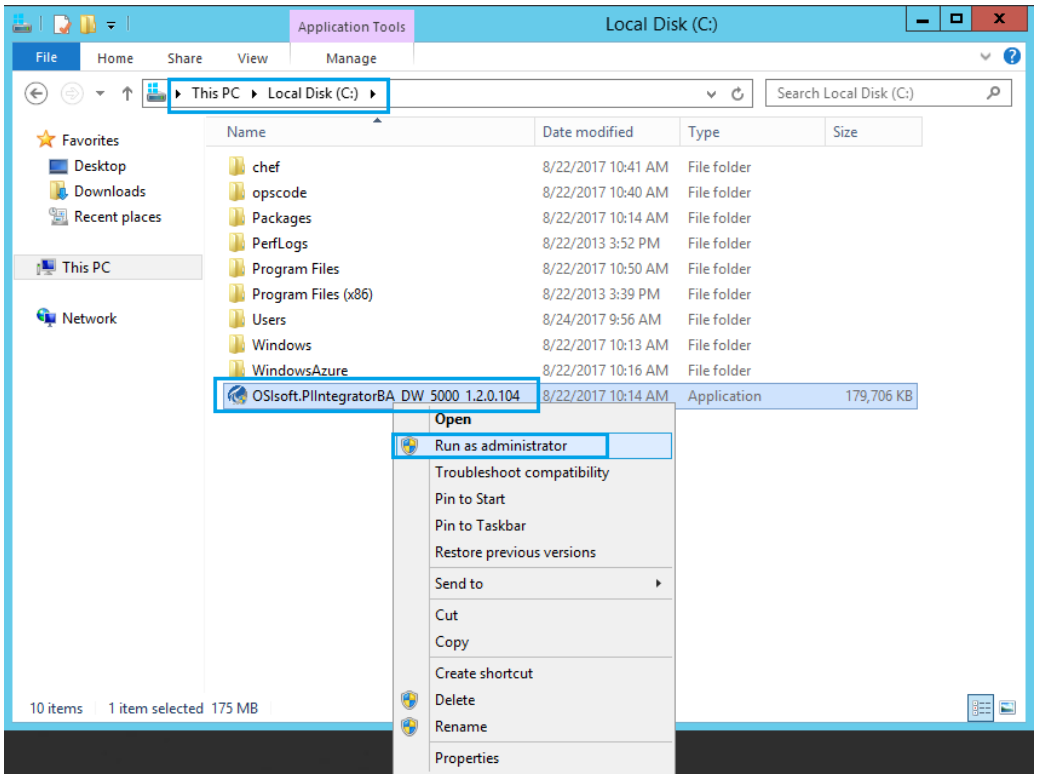


Note: Login with the **same** user credentials you created in the **ADServer**

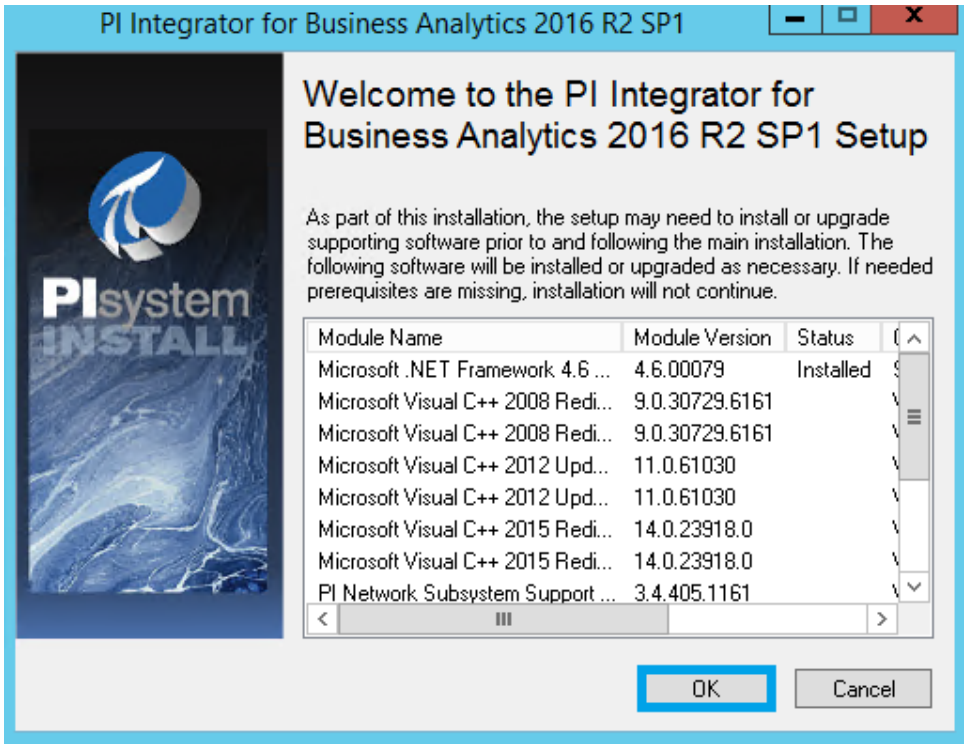
2. Login with credentials**"<domainname>\PIBAInterface"** (user you created in AD server) and aq21**password**.



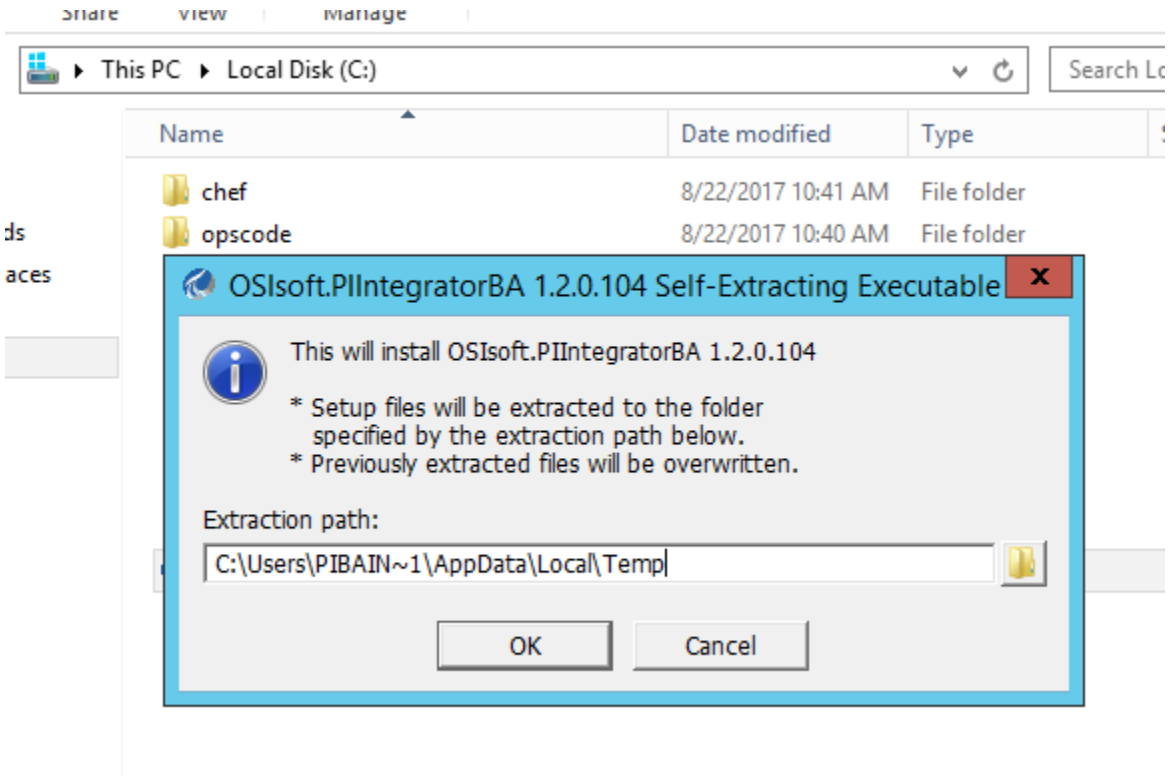
3. After connecting to the PIBA VMServer, navigate to the LocalDisk (C:) and select **OSISoft.PIIntegratorBA,** then right-click on and **Run as adminstrator.**


Application Tools
Local Disk (C:)
File
Home
Share
View
Manage
This PC ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
Type
Size
chef 8/22/2017 10:41 AM File folder
opscode 8/22/2017 10:40 AM File folder
Packages 8/22/2017 10:14 AM File folder
PerfLogs 8/22/2013 3:52 PM File folder
Program Files 8/22/2017 10:50 AM File folder
Program Files (x86) 8/22/2013 3:39 PM File folder
Users 8/24/2017 9:56 AM File folder
Windows 8/22/2017 10:13 AM File folder
WindowsAzure 8/22/2017 10:16 AM File folder
OSIsoft.PIIntegratorBA_DW_5000_1.2.0.104 8/22/2017 10:14 AM Application 179,706 KB
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Pin to Taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
10 items
1 item selected 175 MB

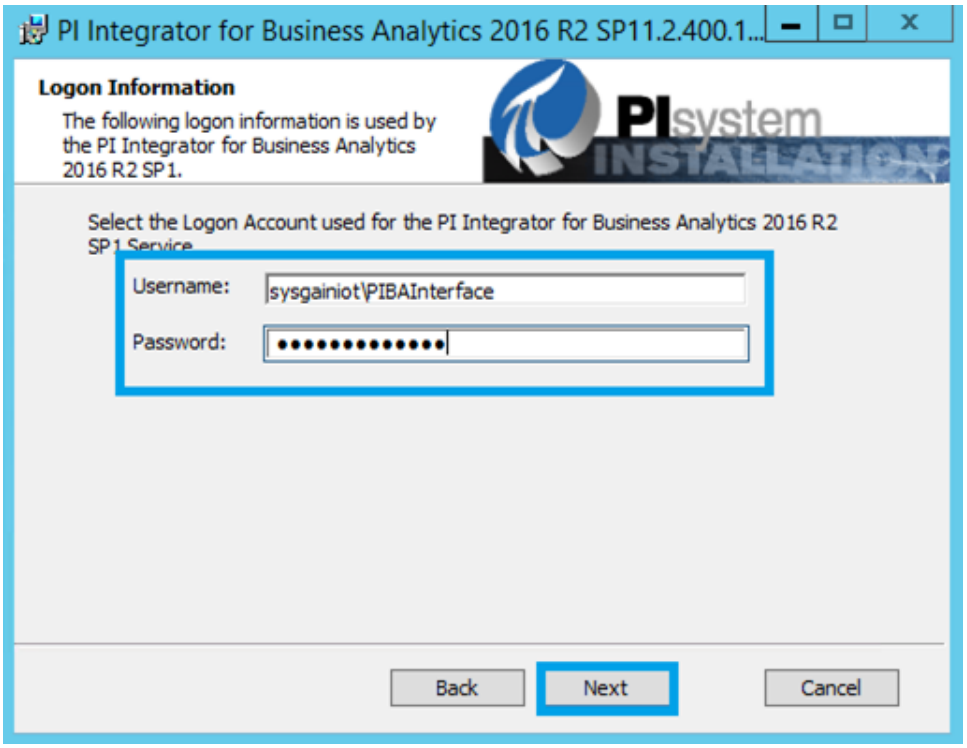
4. Click on **Ok**.


PI Integrator for Business Analytics 2016 R2 SP1
PIsystem
INSTALL
Welcome to the PI Integrator for Business Analytics 2016 R2 SP1 Setup
As part of this installation, the setup may need to install or upgrade supporting software prior to and following the main installation. The following software will be installed or upgraded as necessary. If needed prerequisites are missing, installation will not continue.
Module Name
Module Version
Status
Microsoft .NET Framework 4.6 ... 4.6.00079 Installed
Microsoft Visual C++ 2008 Redi... 9.0.30729.6161
Microsoft Visual C++ 2008 Redi... 9.0.30729.6161
Microsoft Visual C++ 2012 Upd... 11.0.61030
Microsoft Visual C++ 2012 Upd... 11.0.61030
Microsoft Visual C++ 2015 Redi... 14.0.23918.0
Microsoft Visual C++ 2015 Redi... 14.0.23918.0
PI Network Subsystem Support ... 3.4.405.1161
OK
Cancel

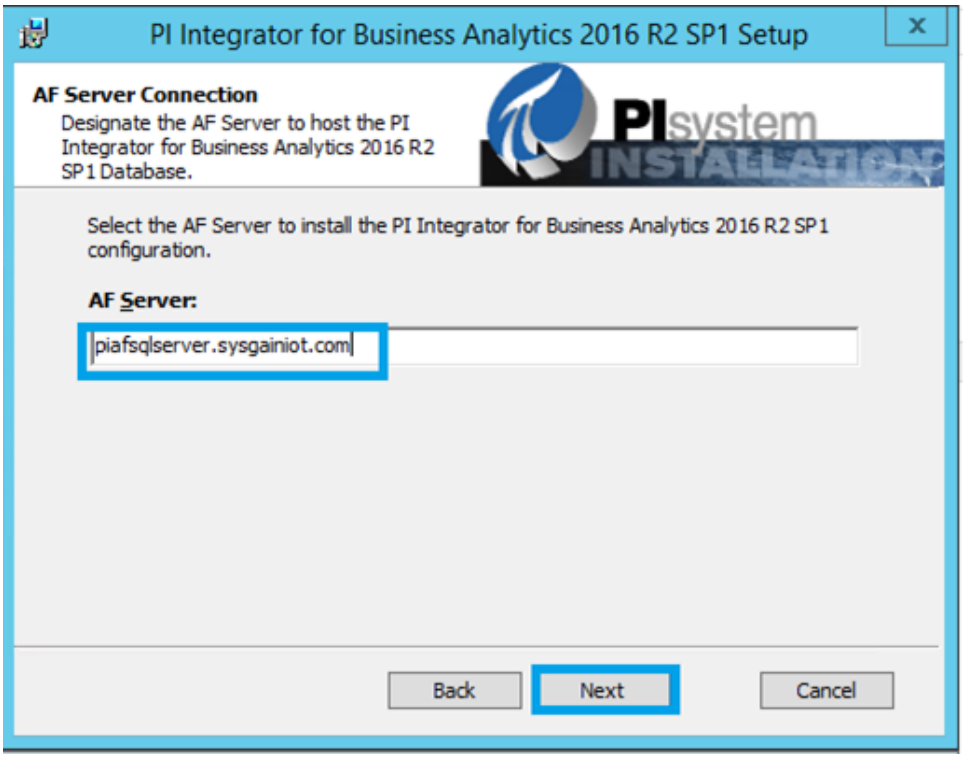
5. Click on **OK**



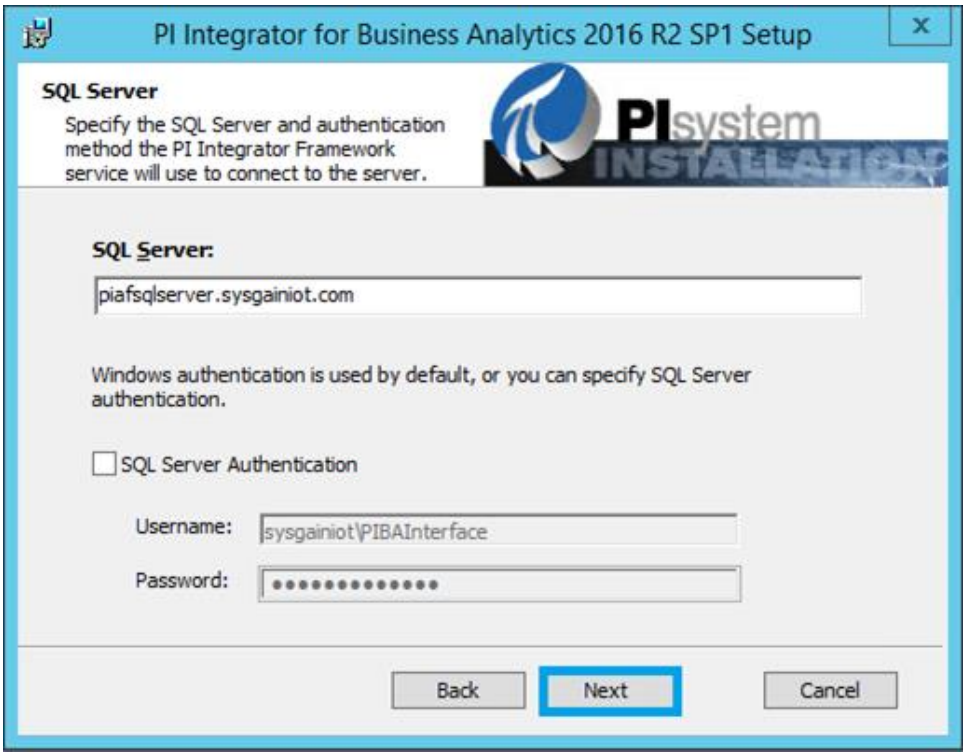
6. Give the same credentials which you used to login to PIBA server in Logon credentials and click on **Next**



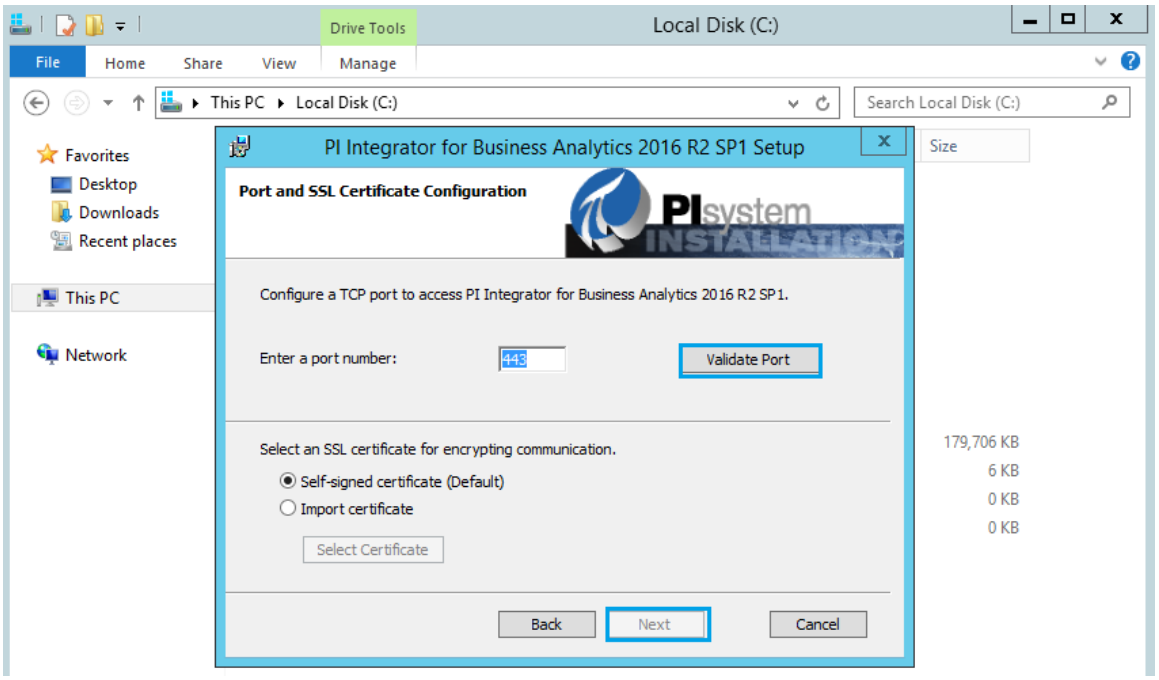
7. Give the AF sever link as piafsqlserver. <domainname> to host PIBA database and lick on **Next**



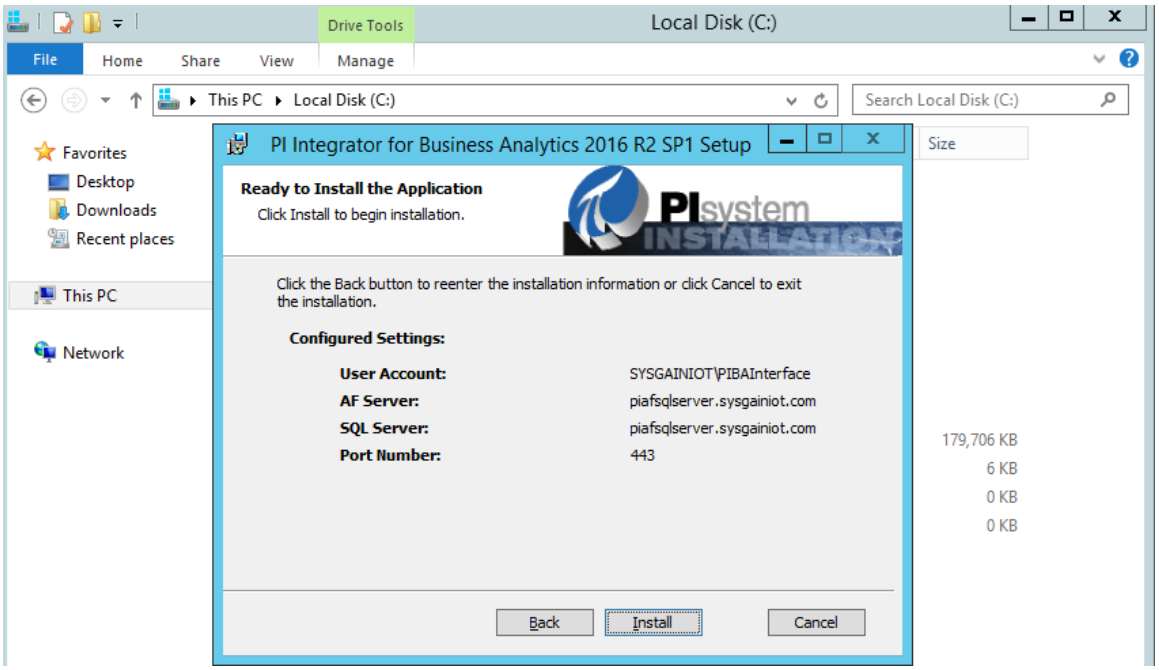
8. Click on **Next**



9. Click on **Validate port,** then **Next.**



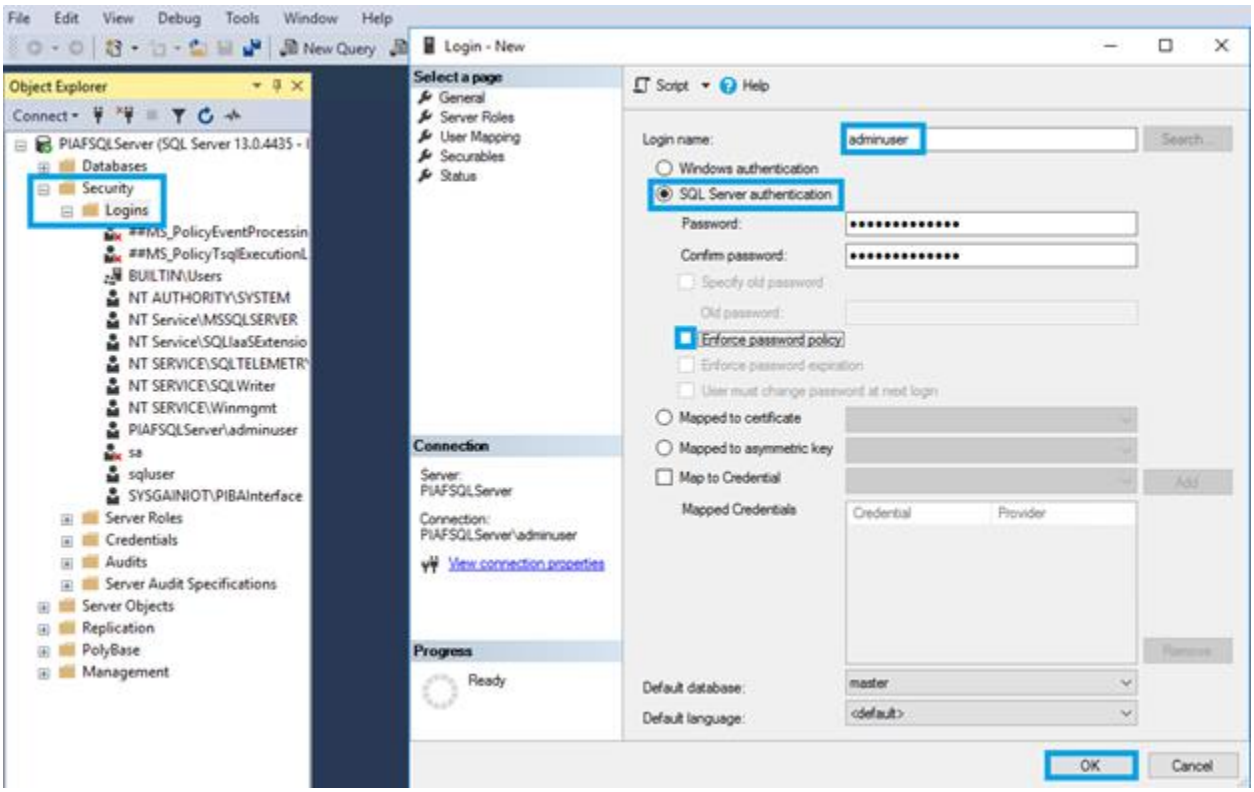
10. Click on **Install.**



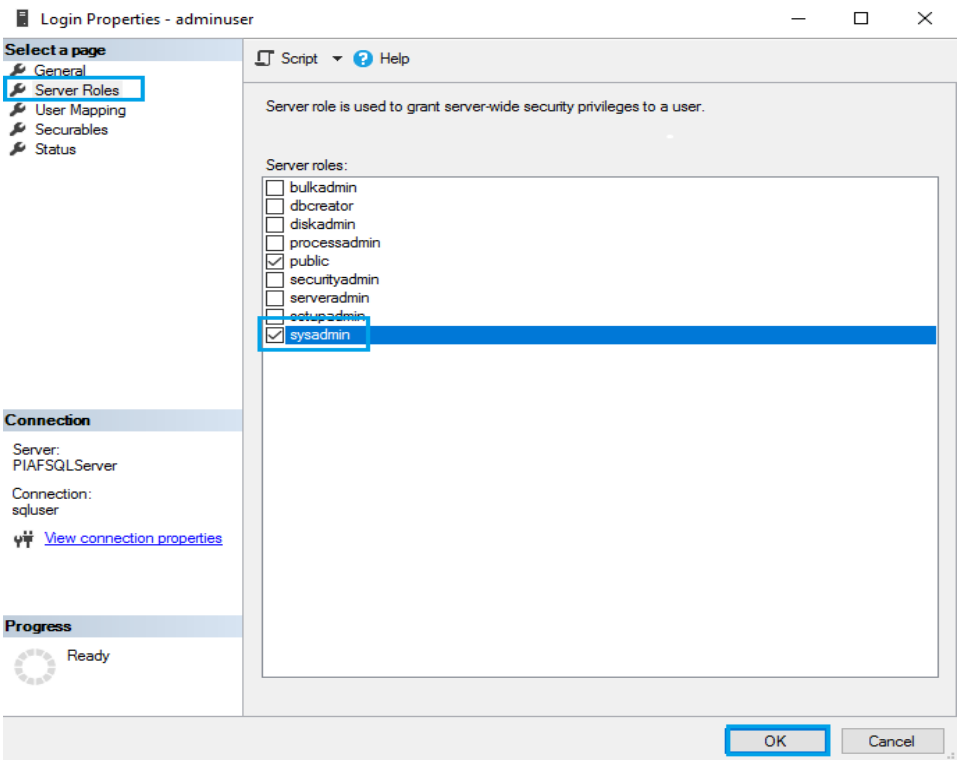
10.1. Configuring PI Business Analytics

1. In Bastion Server, connect to the PIAFSQLServer with the credentials provided in the output section.

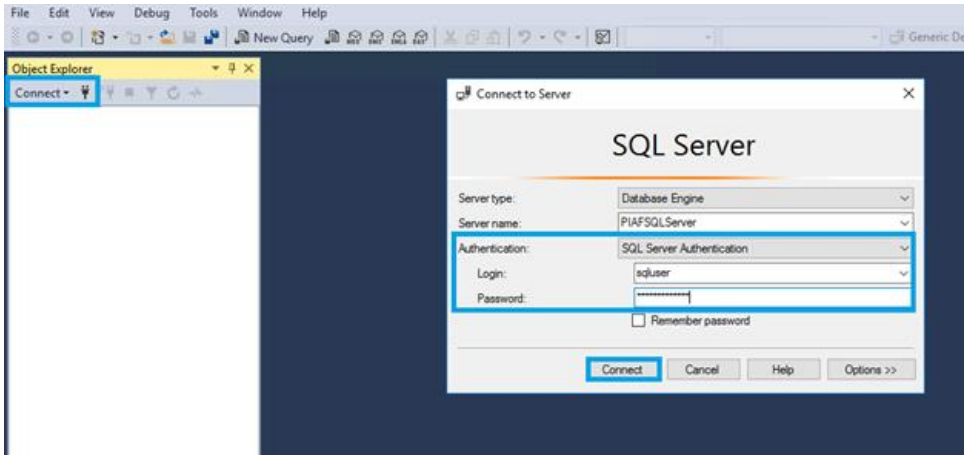
2. Go to the **Security** section, then right-click on **Login** and select **New Login**. Set the login name as **adminuser** and select **SQL Server Authentication.** Set a password and uncheck the box Enforce password policy, then click on **Ok**.



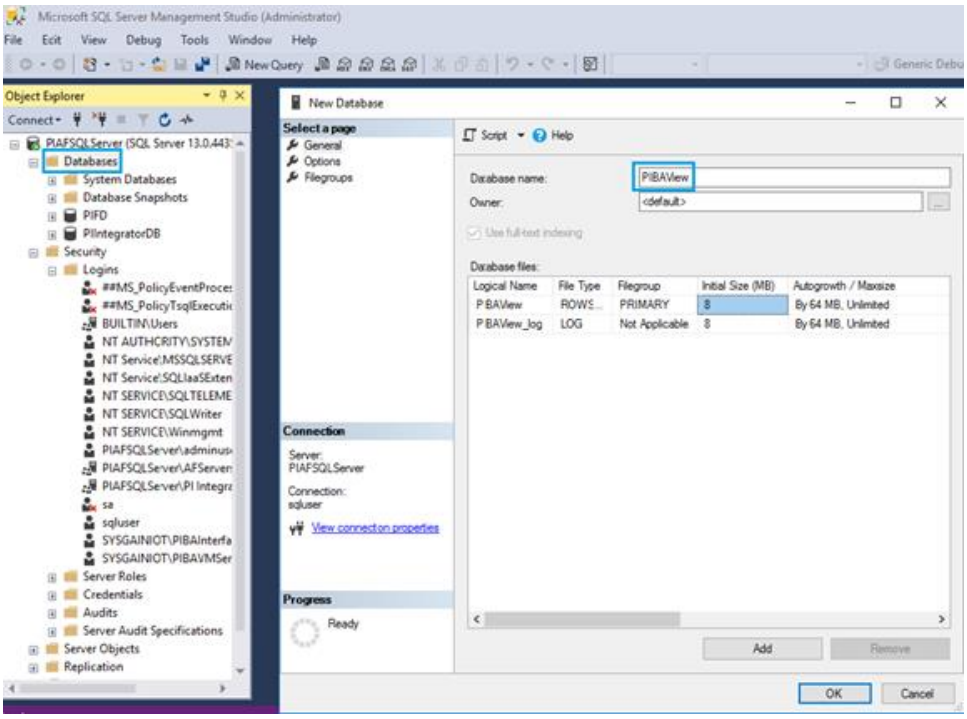
3. Right-click on the admin user under **Login** and select **Properties**. On the Properties screen, select **Server Roles,** then check **sysadmin** and click **Ok**.



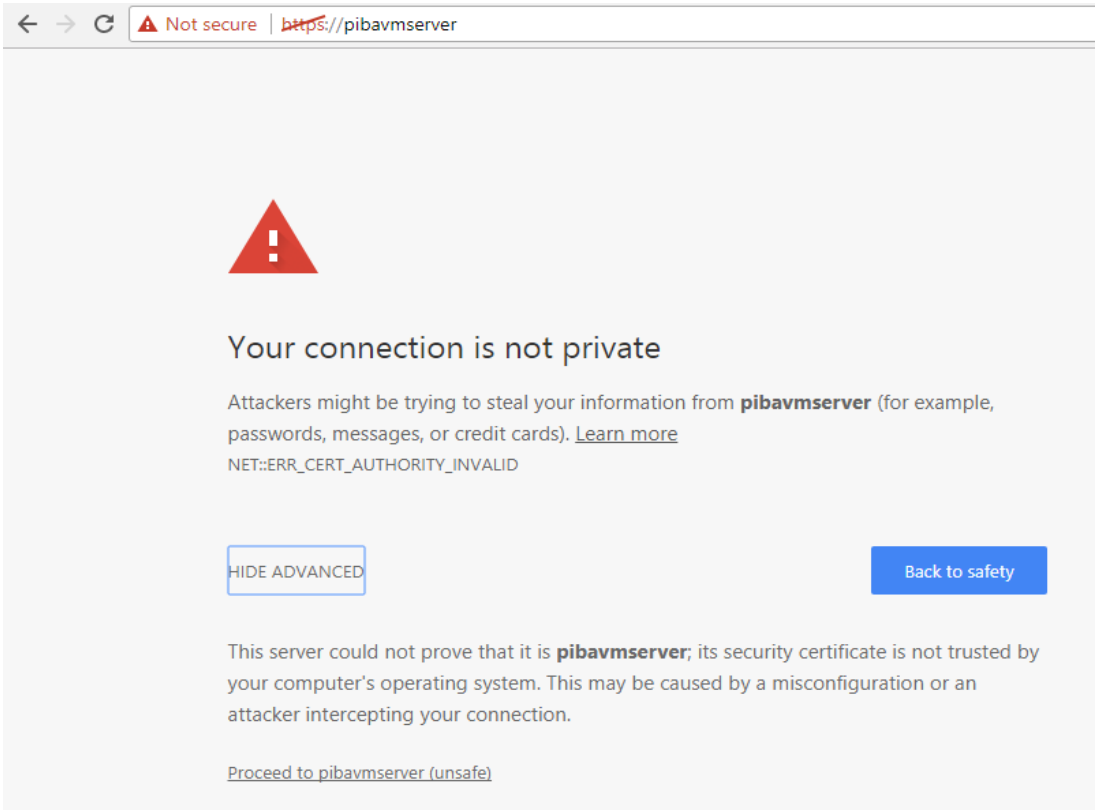
4. Disconnect and Click on connect in **ssms** to login with SQL Server authentication to create database with following SQL credentials



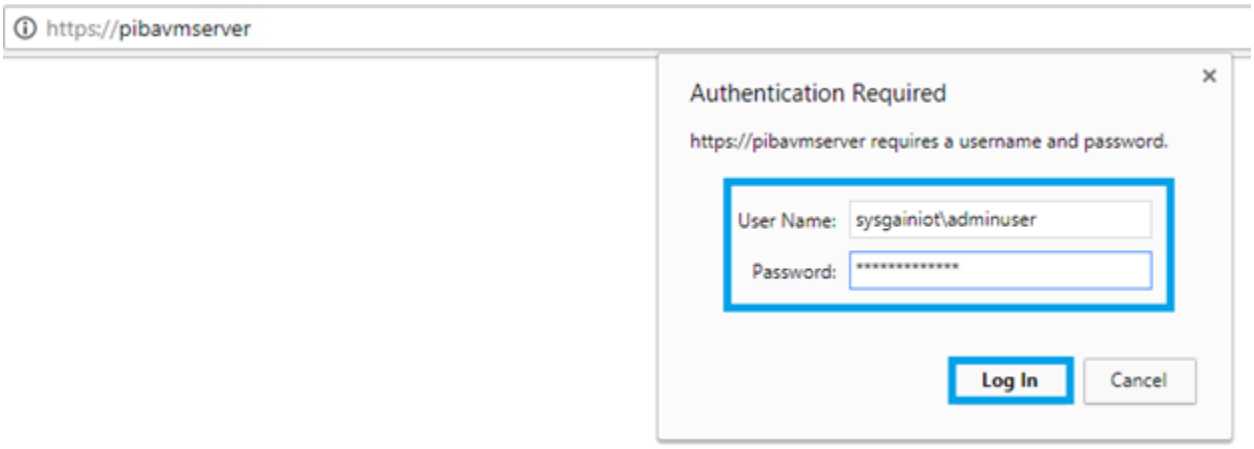
5. Go to the **SQLServer Management Studio**, right-click on **Database**, select **New Database**, and give the Database name as **PIBAView.** Click on **Ok.**



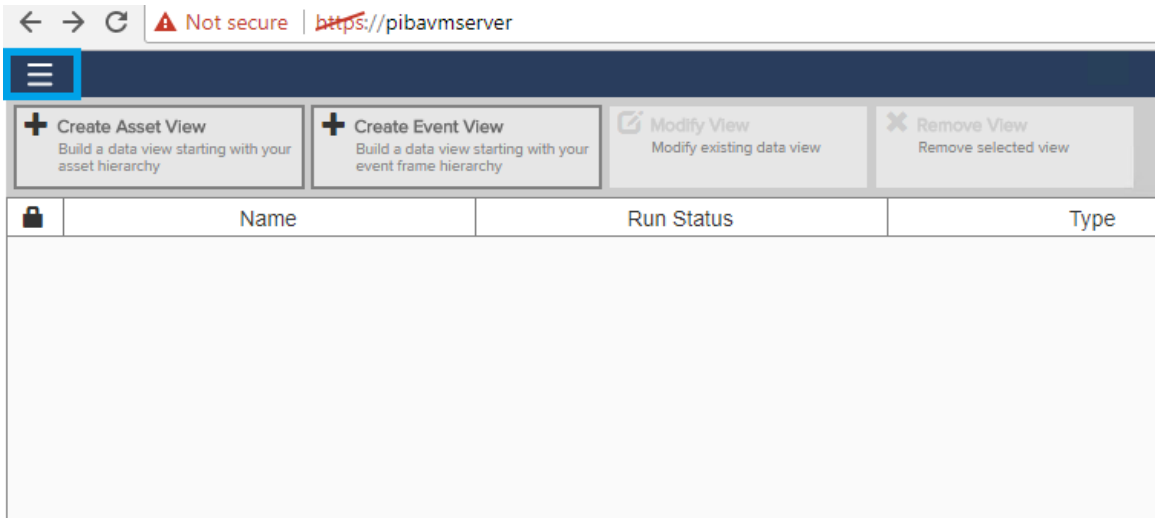
6. Go to the Bastion server: copy and paste https://pibavmserver into a web browser.



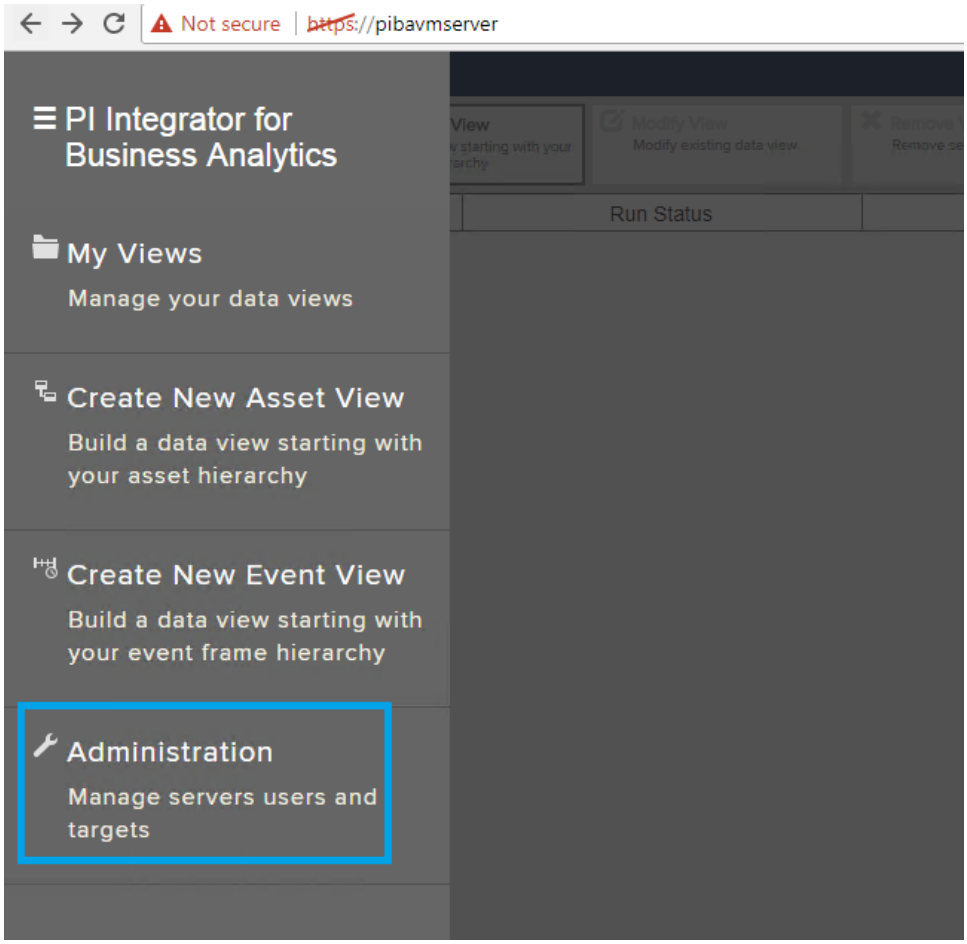
7. Give the credentials as **<domainname>\adminuser** with following password as shown below



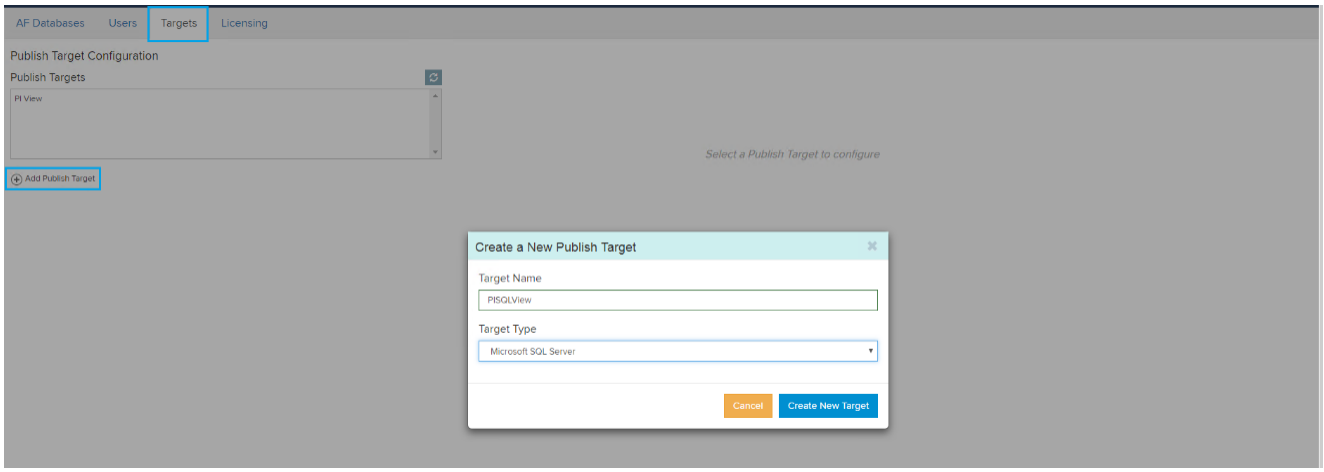
8. Click on **PI Integrator for Business Analytics** as shown below.



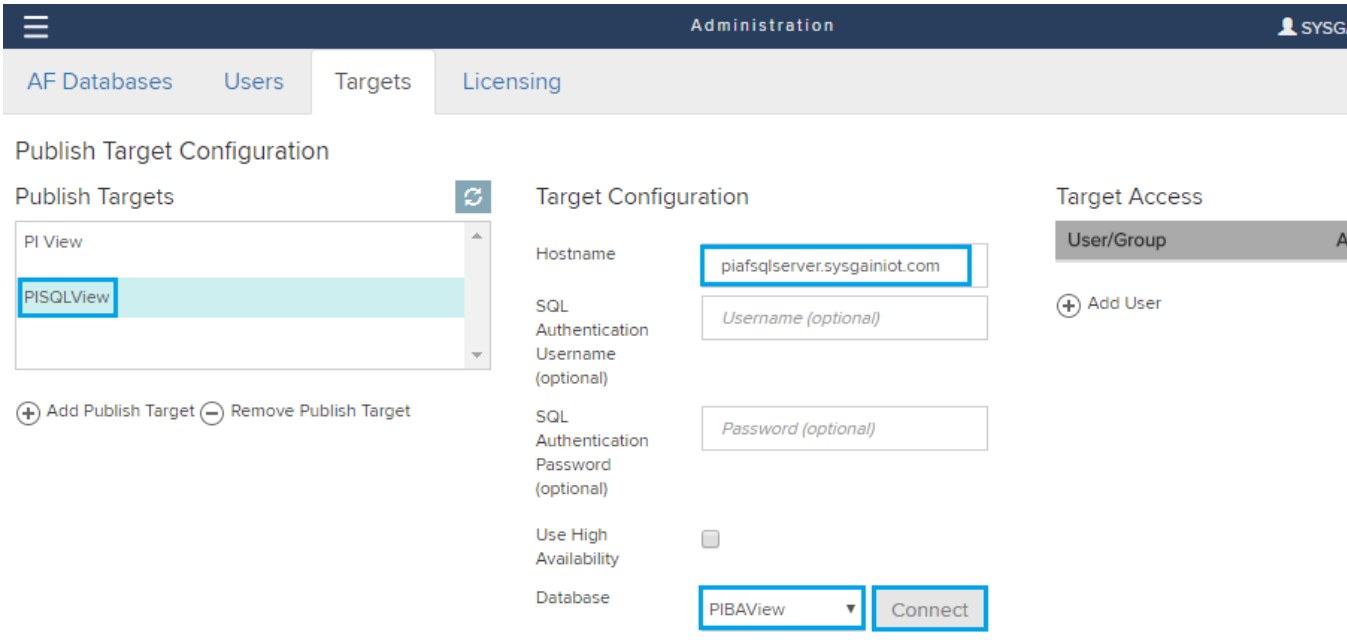
3. Click on **Administration.**



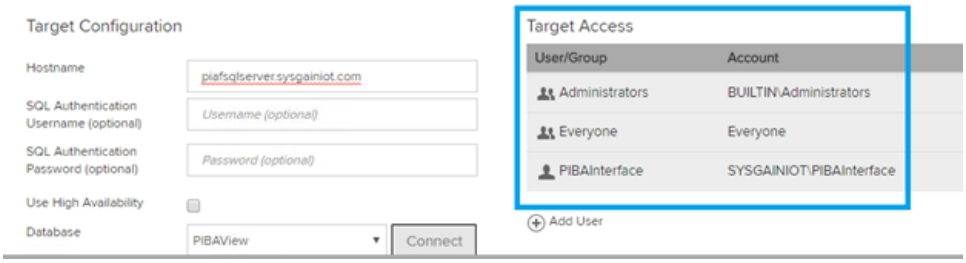
4. Select **Targets** > **Add Publish Target.**
   Enter Target Name as **PISQLView.**
   Select Target type as **Microsoft SQL Server** from drop down. After that click on create new target.



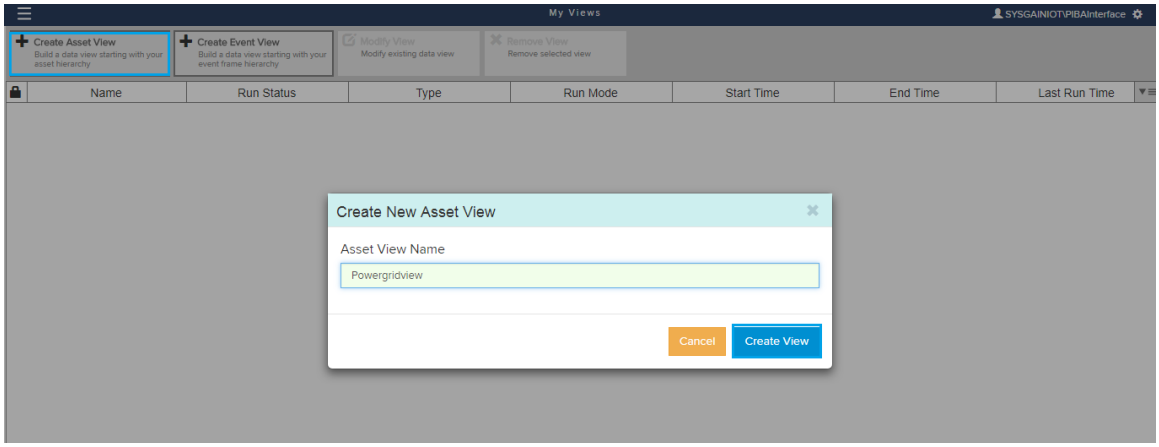
5. Enter the Hostname as **piafsqlserver.<domainname>** and click on connect and then select database you created in piaf ssms, select Database as **PIBAView** and **click on save changes**



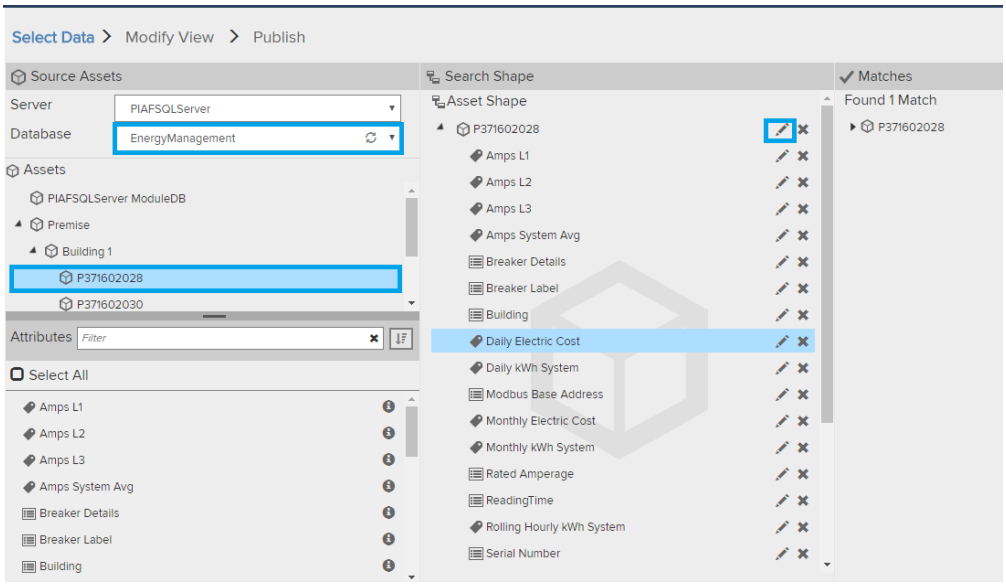
6. You can view the created **target access**



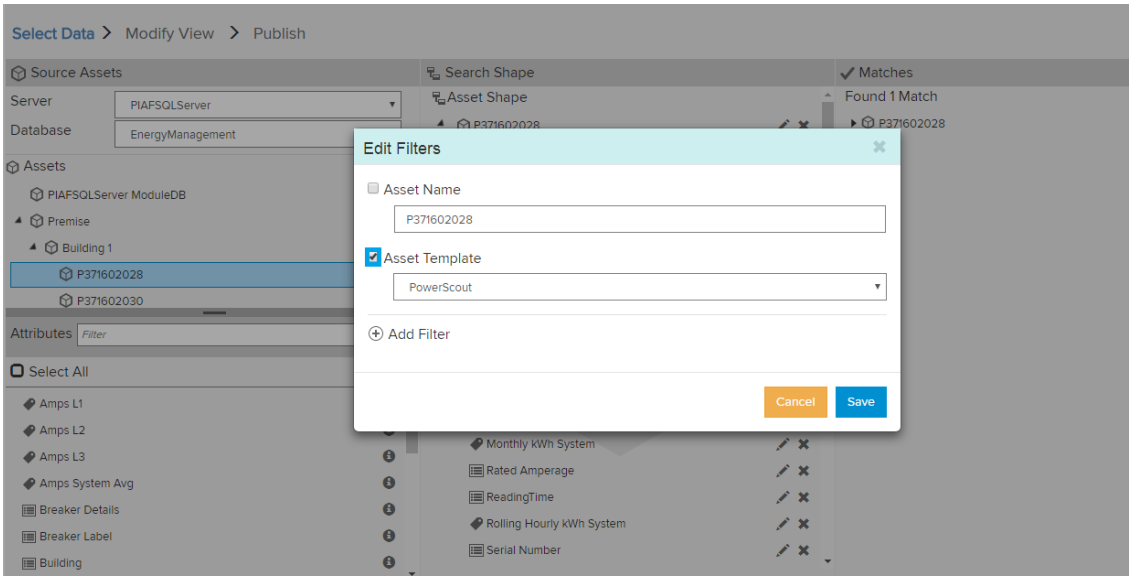
7. Click on **Create Asset view.** Set the Asset View Name as **PowergridView** and click on **Create View.**



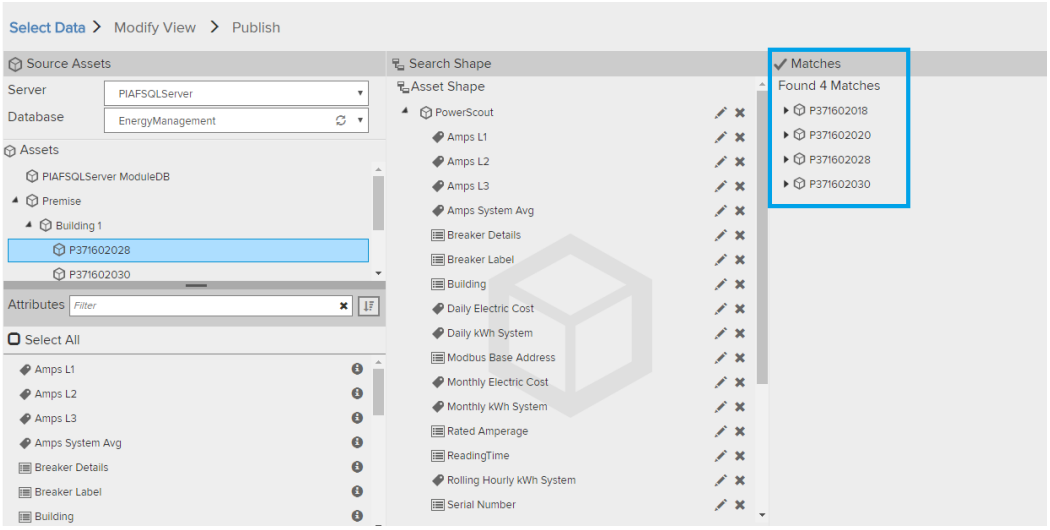
8. Select **EnergyManagement** for Database and select **premise > building1 > any one PI point**. Select all the attributes then drag and drop it under **Asset shape**.



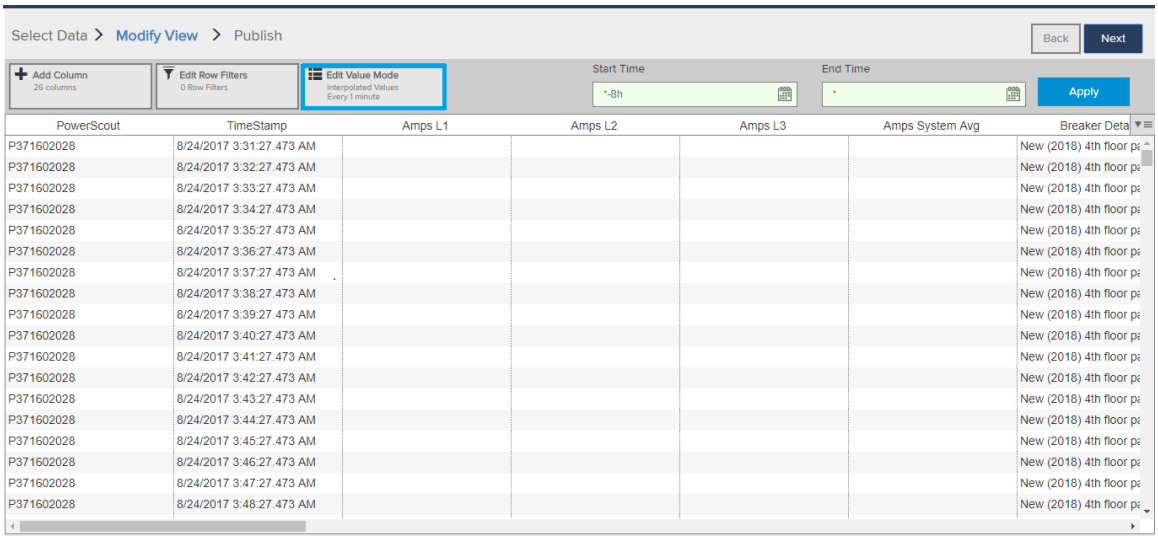
9. Click on edit near PI point **P371602028**, uncheck Asset name box, and check the **Assert Template** and **Save.**



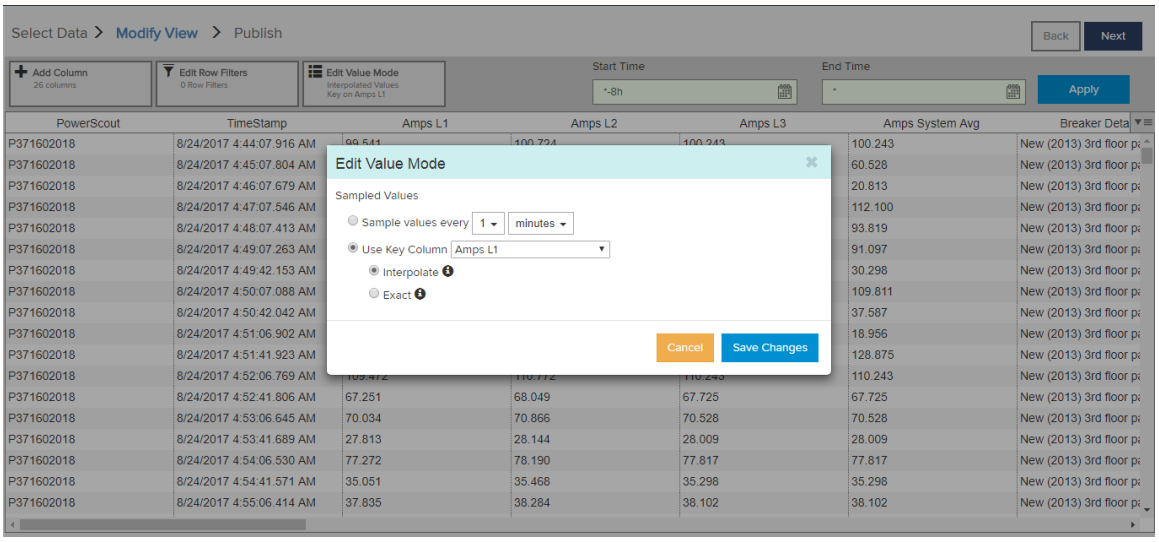
10. You will see the number of matched found on the right-hand side. Then click on **Next.**



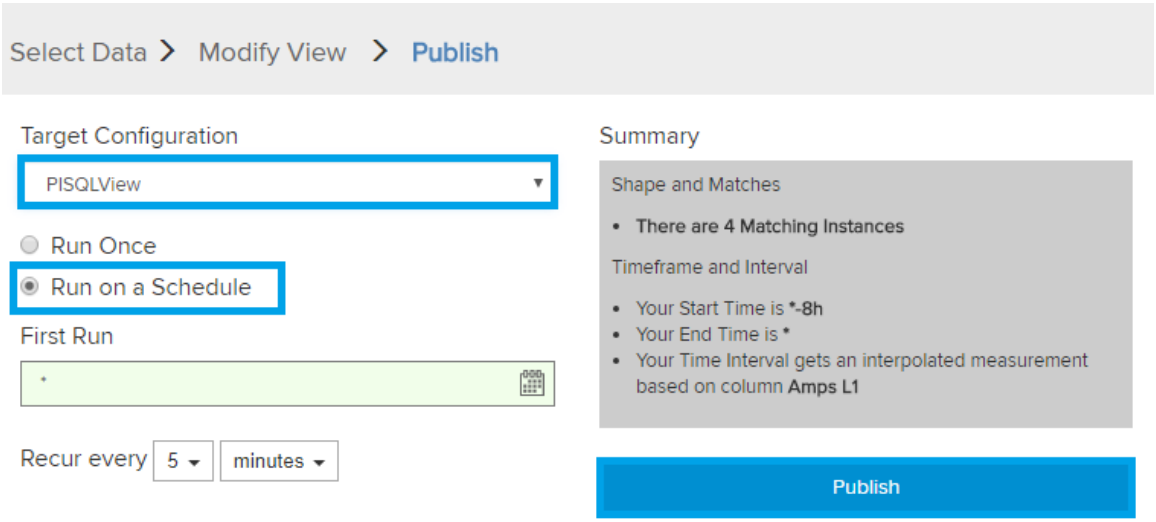
11. Click on **Edit Value Mode**.



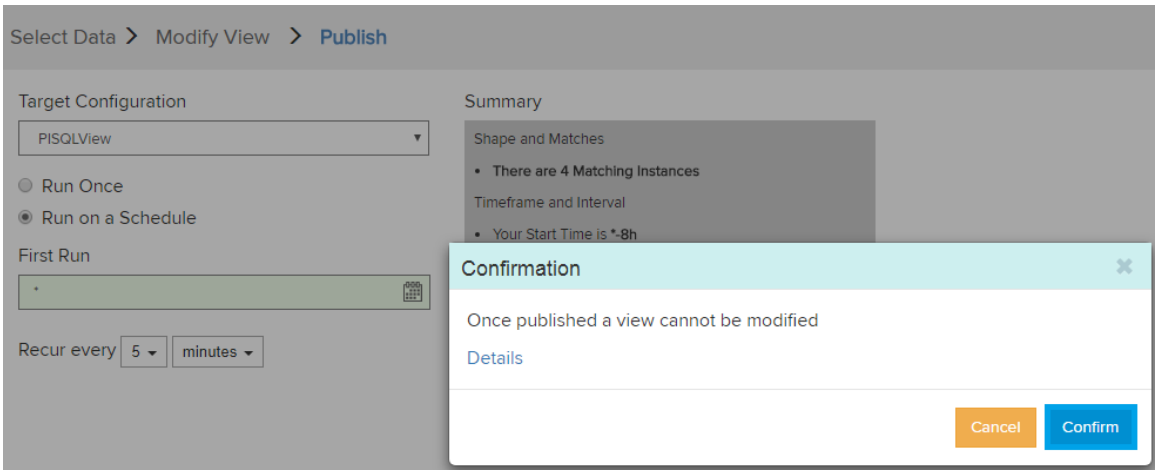
12. Click on **Use Key Column** and **Save Changes**.



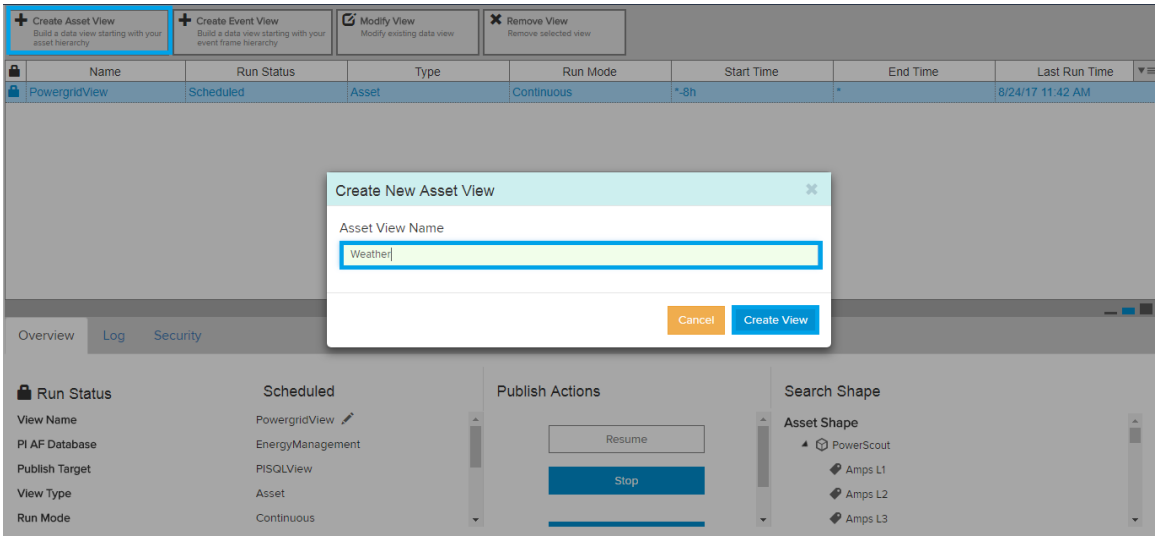
13. Select **PISQLView** for Target configuration, select **Run on a Schedule,** and click on **Publish.**



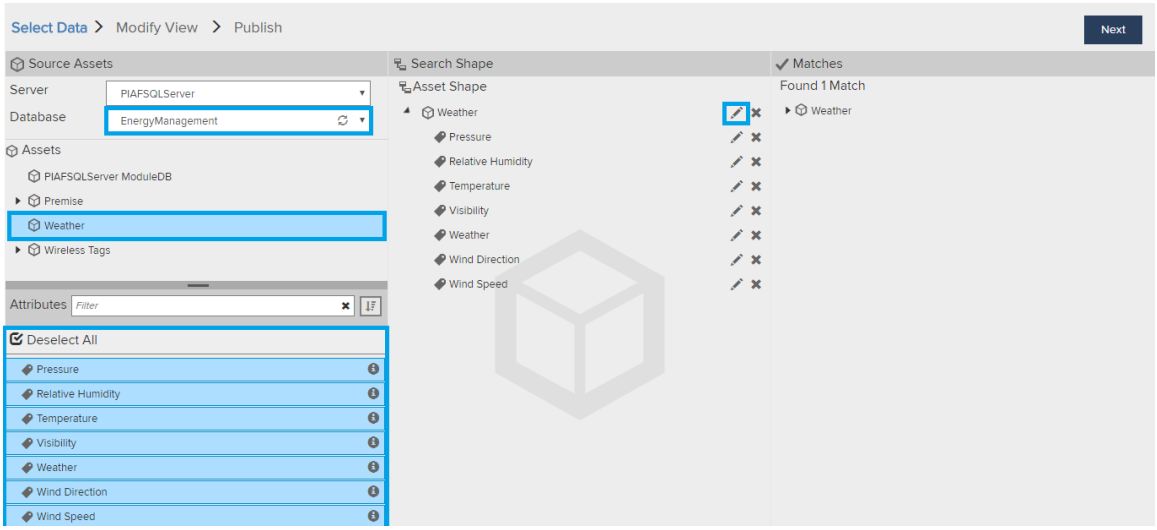
14. Click on **Confirm.**



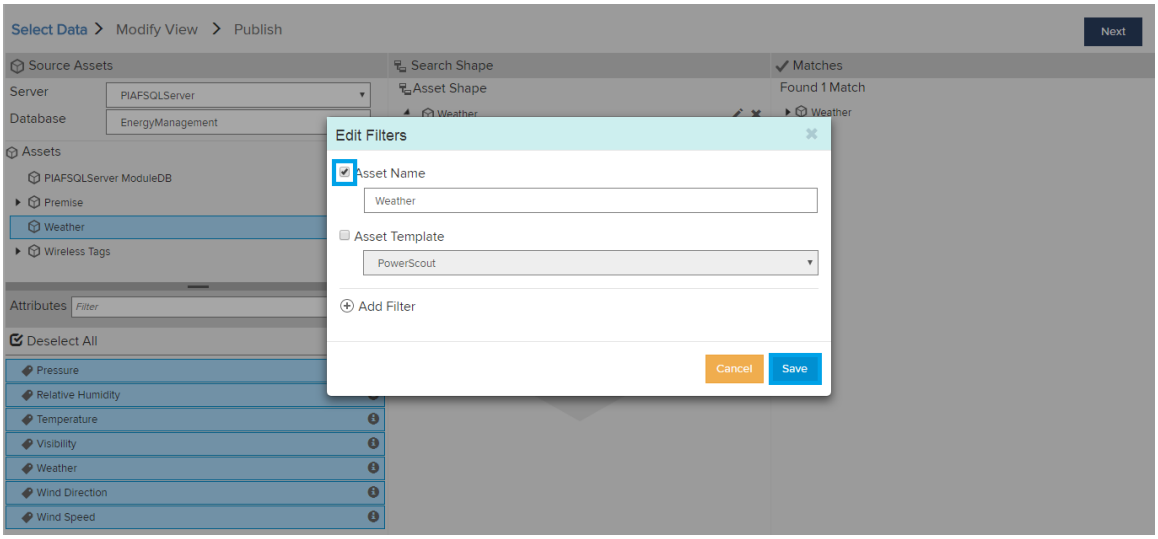
15. Create another Asset view by clicking on **Create asset view**, name it **Weather,** then click on **Create view.**



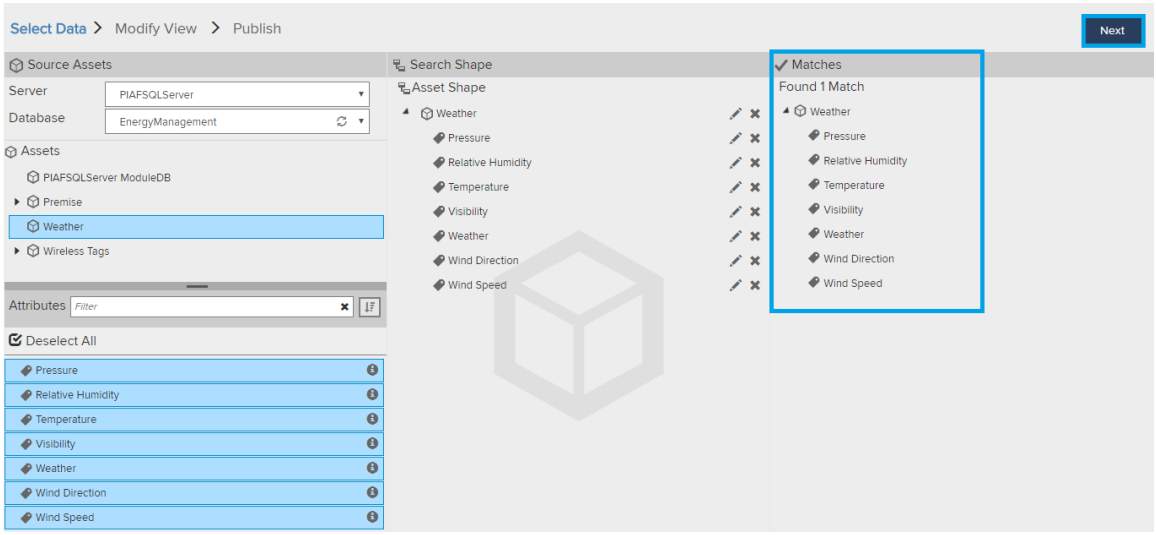
16. Select **Energy management** for Database, click on **Weather**, select all the Attributes, and drag drop the values under Asset Shape.



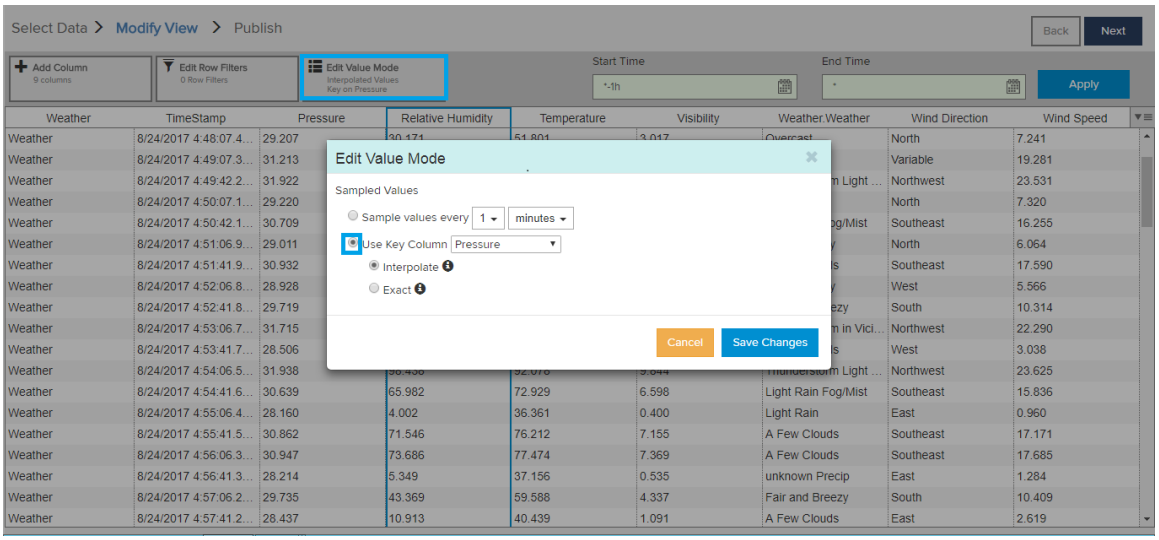
17. Edit the Weather Asset shape, check the box **Asset Name,** and click **Save**.



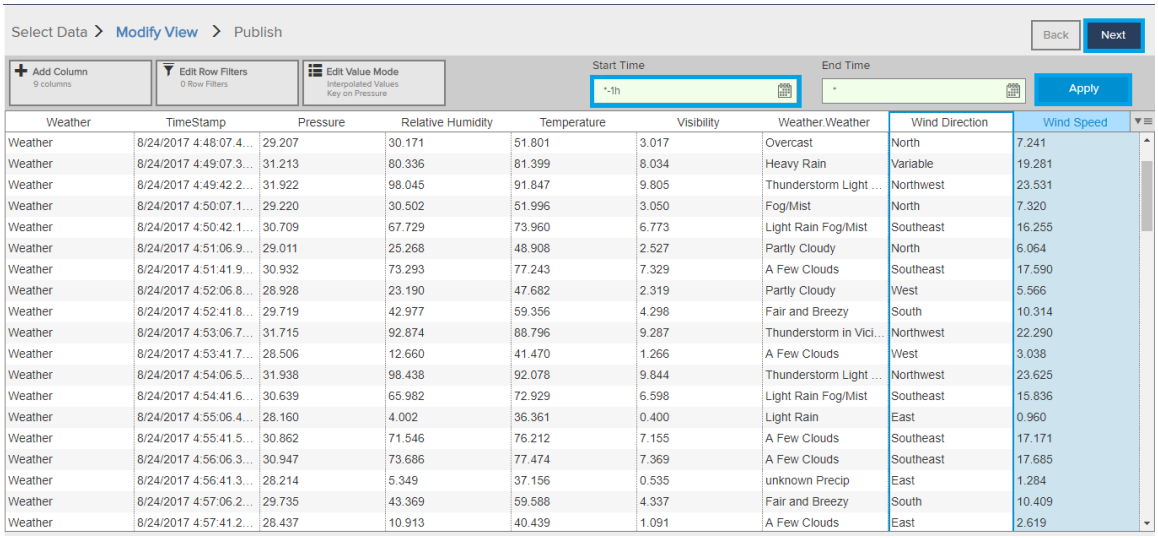
18. The number of matches will appear on the right-hand side.



19. Click on **Edit Value Mode**, select **Use Key Column,** and click **Save Changes**.

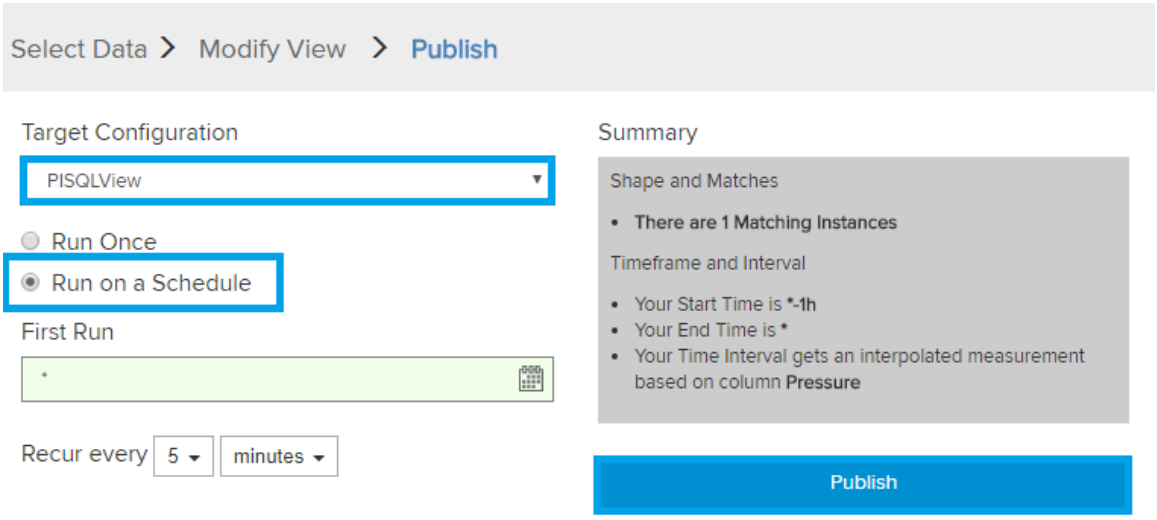


20. Change the start time to ***-1h**, then click **Apply**, and click on **Next.**

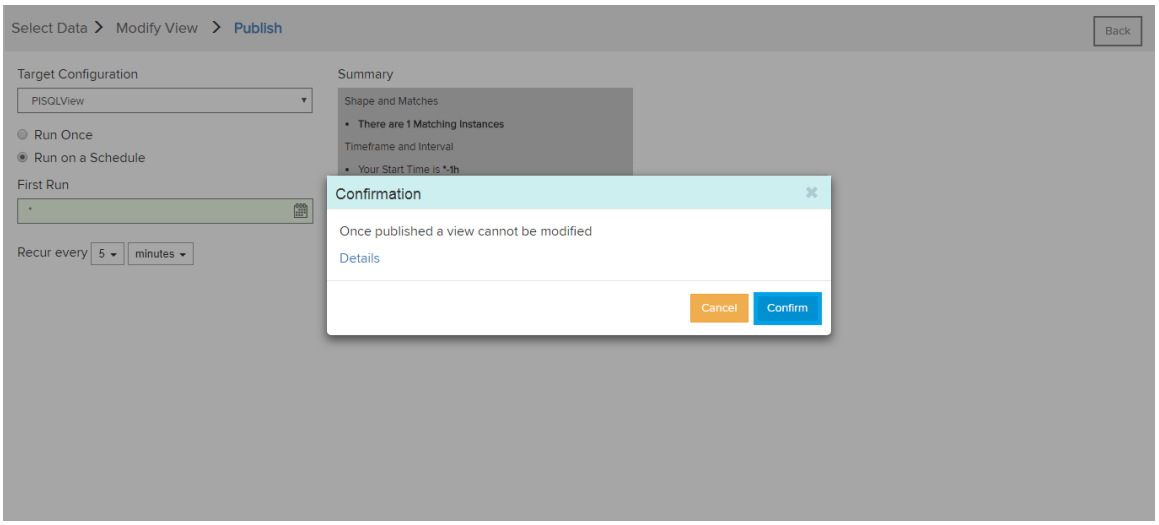


Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather.Weather	Wind Direction	Wind Speed
Weather	8/24/2017 4:48:07.4...	29.207	30.171	51.801	3.017	Overcast	North	7.241
Weather	8/24/2017 4:49:07.3...	31.213	80.336	81.399	8.034	Heavy Rain	Variable	19.281
Weather	8/24/2017 4:49:42.2...	31.922	98.045	91.847	9.805	Thunderstorm Light ...	Northwest	23.531
Weather	8/24/2017 4:50:07.1...	29.220	30.502	51.996	3.050	Fog/Mist	North	7.320
Weather	8/24/2017 4:50:42.1...	30.709	67.729	73.960	6.773	Light Rain Fog/Mist	Southeast	16.255
Weather	8/24/2017 4:51:06.9...	29.011	25.268	48.908	2.527	Partly Cloudy	North	6.064
Weather	8/24/2017 4:51:41.9...	30.932	73.293	77.243	7.329	A Few Clouds	Southeast	17.590
Weather	8/24/2017 4:52:06.8...	28.928	23.190	47.682	2.319	Partly Cloudy	West	5.566
Weather	8/24/2017 4:52:41.8...	29.719	42.977	59.356	4.298	Fair and Breezy	South	10.314
Weather	8/24/2017 4:53:06.7...	31.715	92.874	88.796	9.287	Thunderstorm in Vici...	Northwest	22.290
Weather	8/24/2017 4:53:41.7...	28.506	12.660	41.470	1.266	A Few Clouds	West	3.038
Weather	8/24/2017 4:54:06.5...	31.938	98.438	92.078	9.844	Thunderstorm Light ...	Northwest	23.625
Weather	8/24/2017 4:54:41.6...	30.639	65.982	72.929	6.598	Light Rain Fog/Mist	Southeast	15.836
Weather	8/24/2017 4:55:06.4...	28.160	4.002	36.361	0.400	Light Rain	East	0.960
Weather	8/24/2017 4:55:41.5...	30.862	71.546	76.212	7.155	A Few Clouds	Southeast	17.171
Weather	8/24/2017 4:56:06.3...	30.947	73.686	77.474	7.369	A Few Clouds	Southeast	17.685
Weather	8/24/2017 4:56:41.3...	28.214	5.349	37.156	0.535	unknown Precip	East	1.284
Weather	8/24/2017 4:57:06.2...	29.735	43.369	59.588	4.337	Fair and Breezy	South	10.409
Weather	8/24/2017 4:57:41.2...	28.437	10.913	40.439	1.091	A Few Clouds	East	2.619

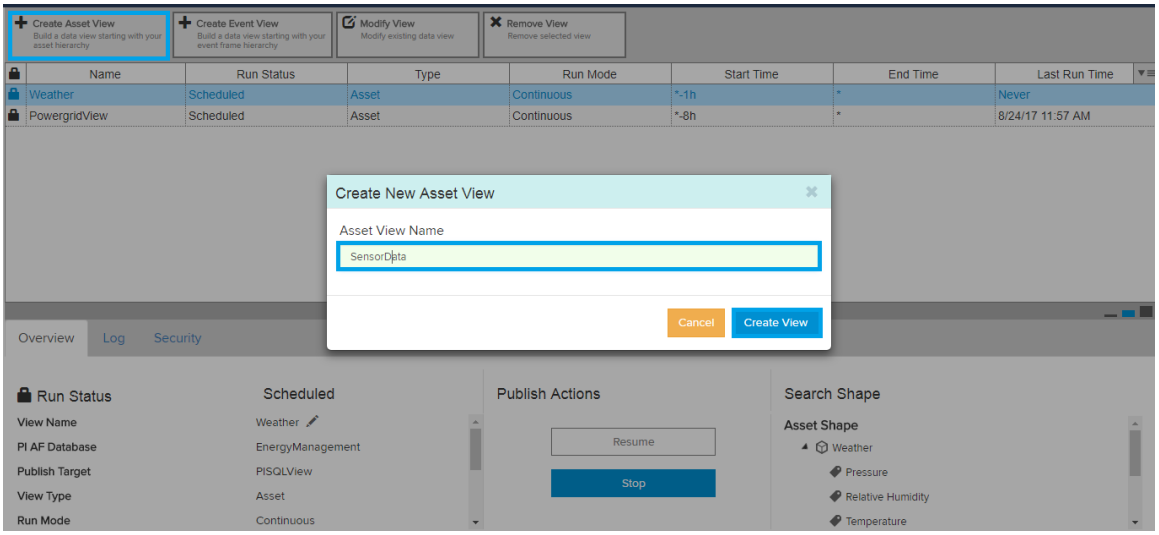
21. Select **PISQLView** under Target Configuration and select **Run on Schedule,** then click **Publish.**



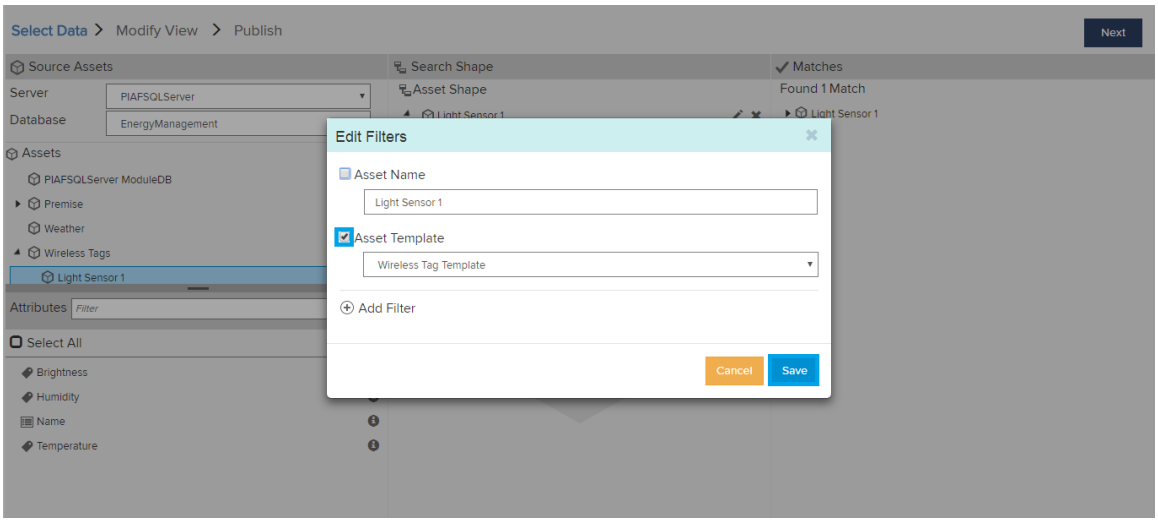
22. Click on **Confirm.**



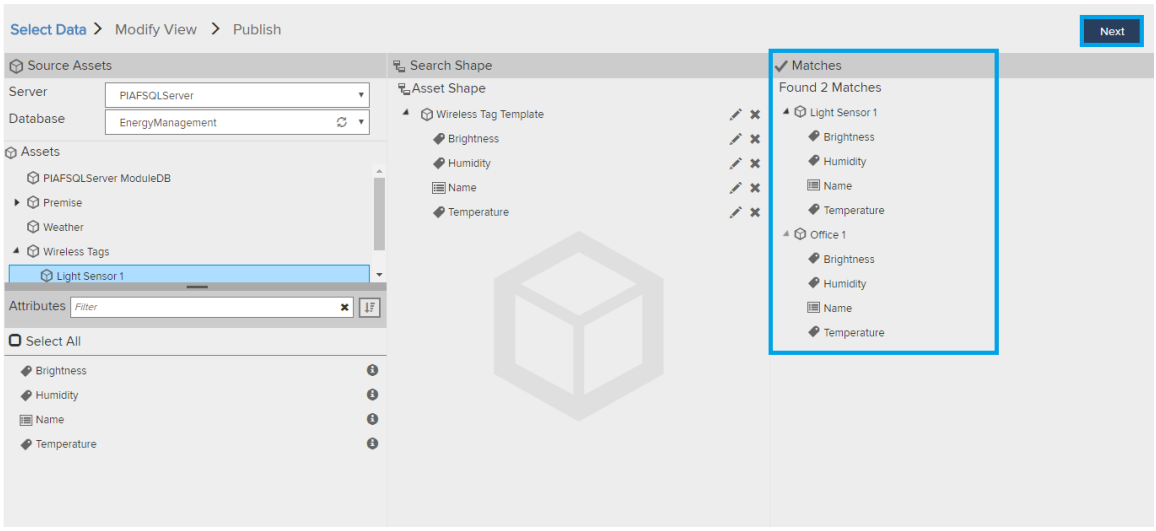
23. Create another Asset view with the name **SensorData** and click on **Create View**.



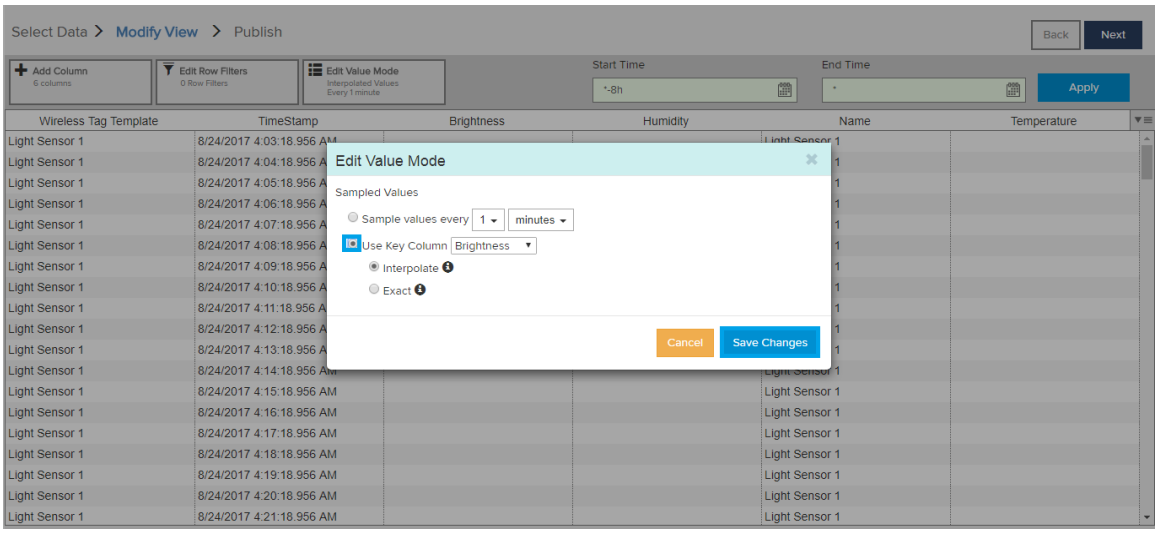
24. Click on **Edit** on Light sensor, then check the box **Asset template** and click **Save**.



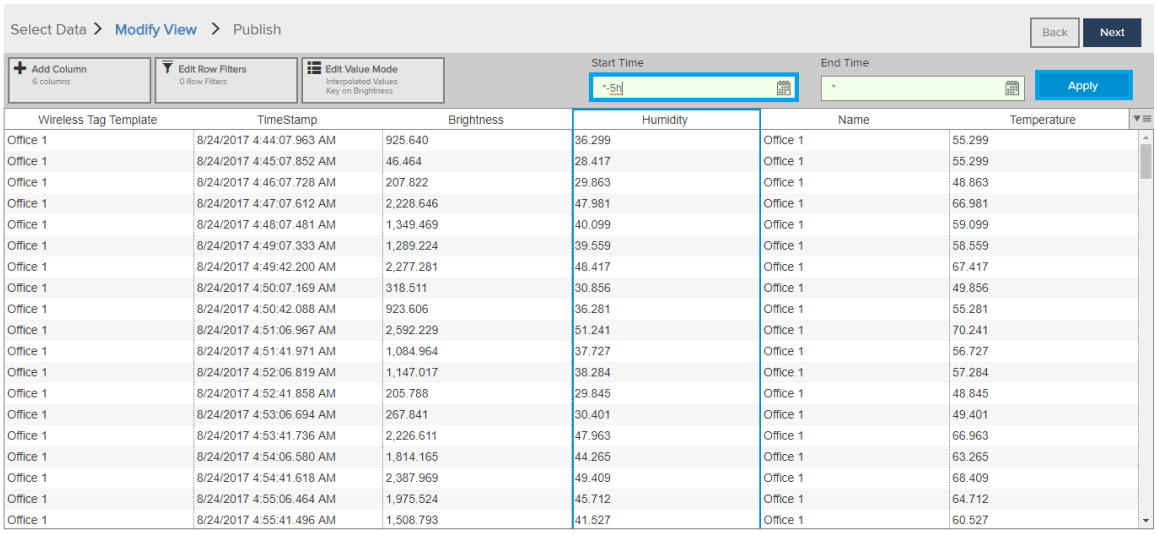
25. The matches will appear on the right-hand side and click on **Next**



26. Click on **Edit Value Mode**, select **Use Key Column,** and **Save Changes.**

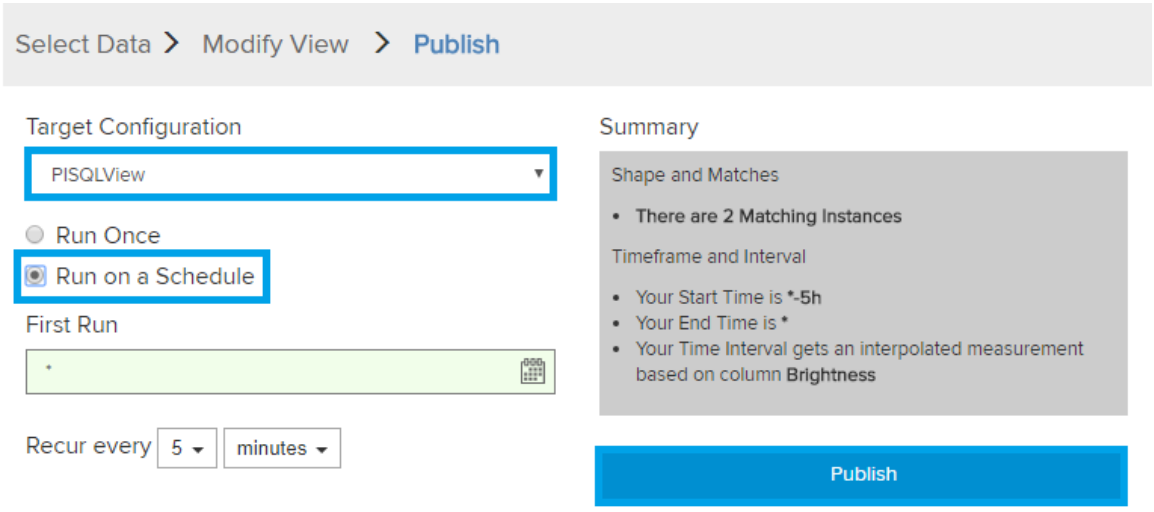


27. Select the start time as ***-5h**, then click **Apply** and click **Next.**

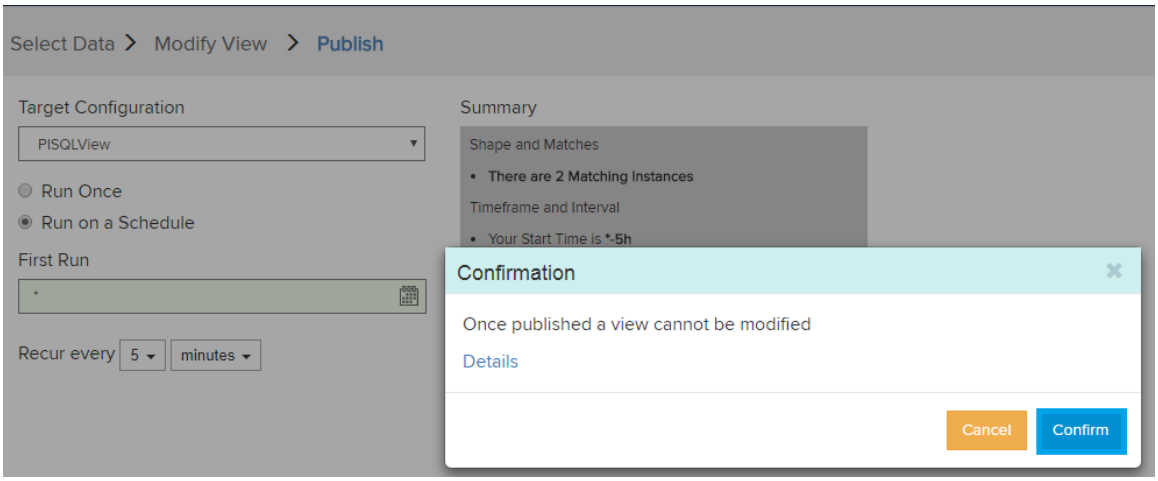


Wireless Tag Template	TimeStamp	Brightness	Humidity	Name	Temperature
Office 1	8/24/2017 4:44:07.963 AM	925.640	36.299	Office 1	55.299
Office 1	8/24/2017 4:45:07.852 AM	46.464	28.417	Office 1	55.299
Office 1	8/24/2017 4:46:07.728 AM	207.822	29.863	Office 1	48.863
Office 1	8/24/2017 4:47:07.612 AM	2,228.646	47.981	Office 1	66.981
Office 1	8/24/2017 4:48:07.481 AM	1,349.469	40.099	Office 1	59.099
Office 1	8/24/2017 4:49:07.333 AM	1,289.224	39.559	Office 1	58.559
Office 1	8/24/2017 4:49:42.200 AM	2,277.281	48.417	Office 1	67.417
Office 1	8/24/2017 4:50:07.169 AM	318.511	30.856	Office 1	49.856
Office 1	8/24/2017 4:50:42.088 AM	923.606	36.281	Office 1	55.281
Office 1	8/24/2017 4:51:06.967 AM	2,592.229	51.241	Office 1	70.241
Office 1	8/24/2017 4:51:41.971 AM	1,084.964	37.727	Office 1	56.727
Office 1	8/24/2017 4:52:06.819 AM	1,147.017	38.284	Office 1	57.284
Office 1	8/24/2017 4:52:41.858 AM	205.788	29.845	Office 1	48.845
Office 1	8/24/2017 4:53:06.694 AM	267.841	30.401	Office 1	49.401
Office 1	8/24/2017 4:53:41.736 AM	2,226.611	47.963	Office 1	66.963
Office 1	8/24/2017 4:54:06.580 AM	1,814.165	44.265	Office 1	63.265
Office 1	8/24/2017 4:54:41.618 AM	2,387.969	49.409	Office 1	68.409
Office 1	8/24/2017 4:55:06.464 AM	1,975.524	45.712	Office 1	64.712
Office 1	8/24/2017 4:55:41.496 AM	1,508.793	41.527	Office 1	60.527

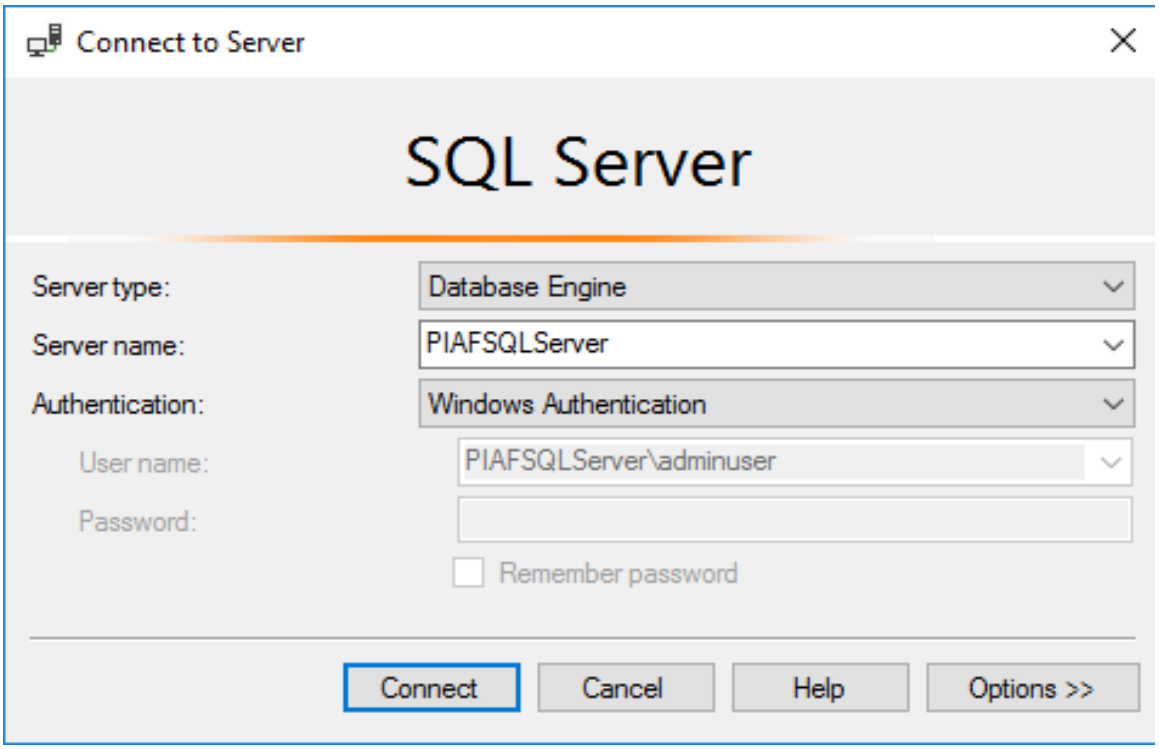
28. Select **PISQlView** under Target Configuration and click on **Run on a Schedule,** then click **Publish.**



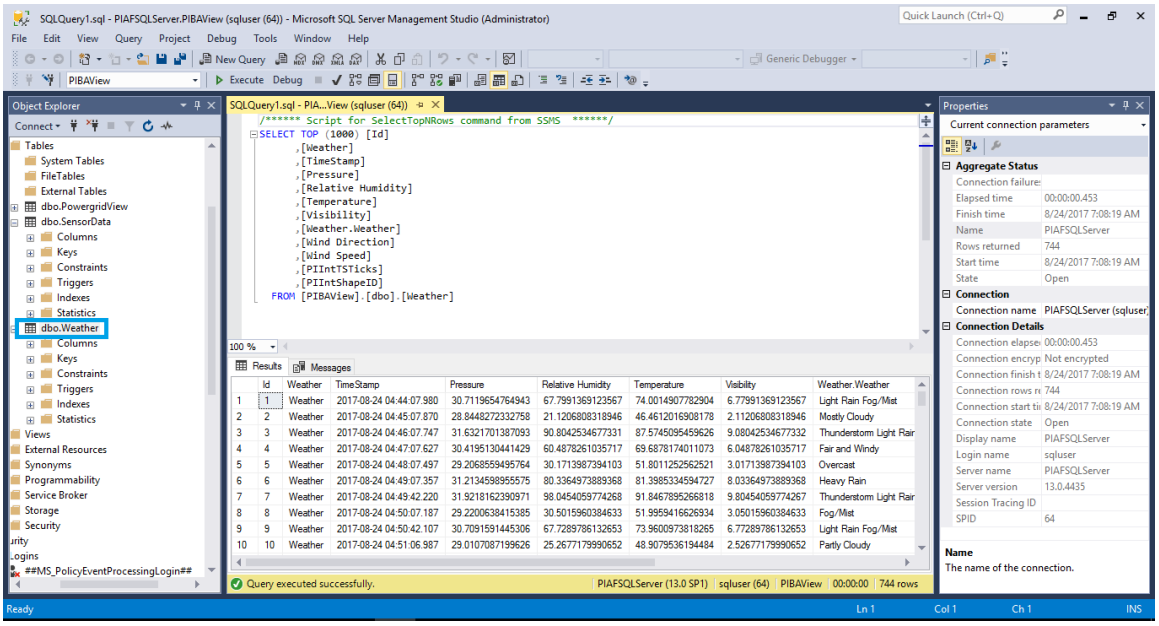
29. Click on **Confirm**.



30. After creating the Asset Views, check in **PISQLAFServer** in **SQL Server Management Studio**.

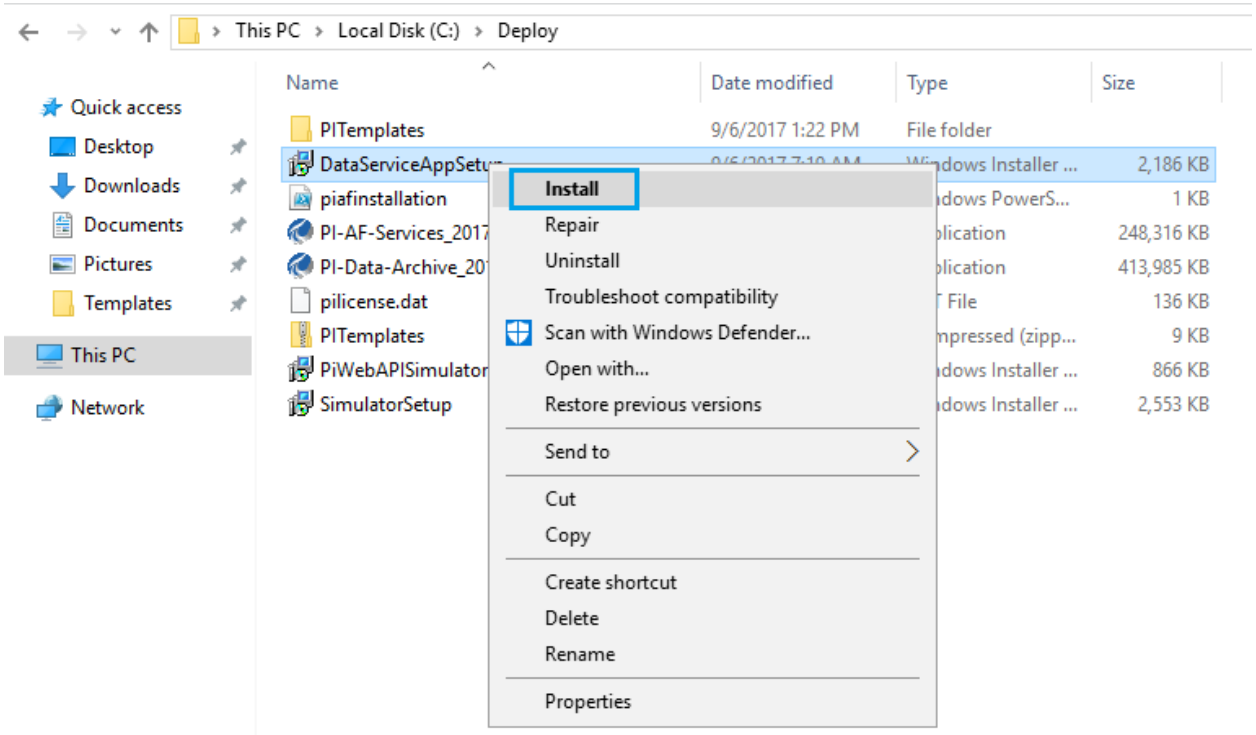


31. you must navigate to the **PIBAView** database > **Tables** and right click on any of the tables, then click on **Select Top 1000 Rows.**

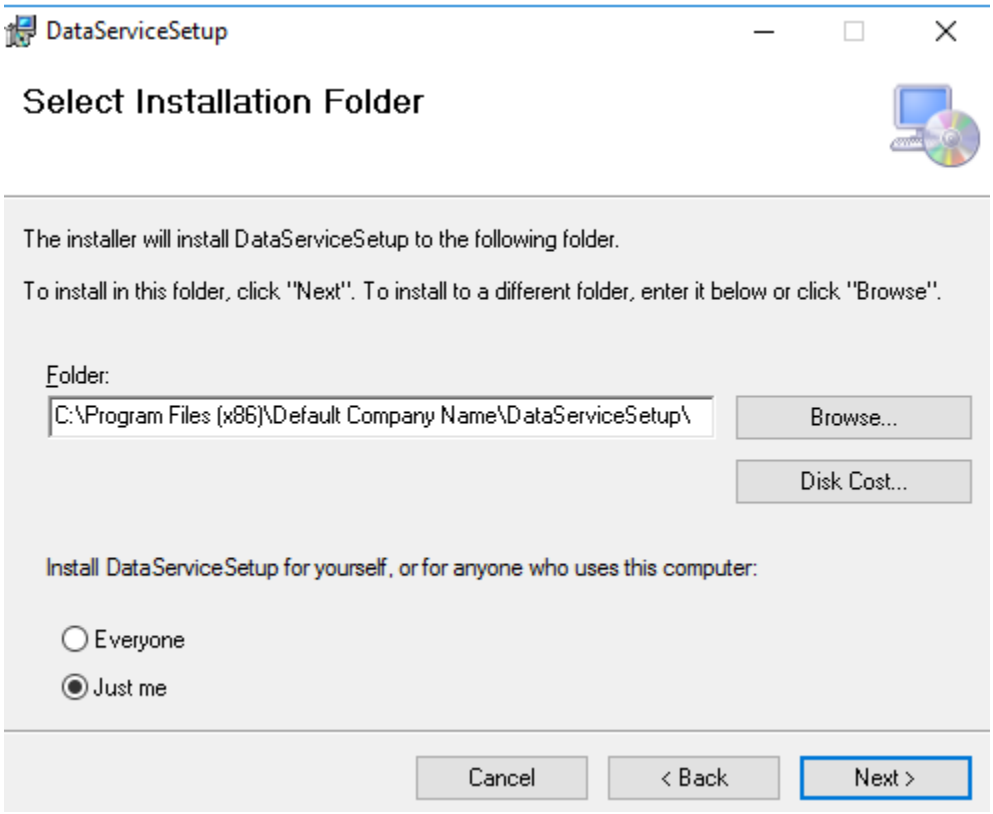


10.2. Install And Run The DataServiceAppSetup

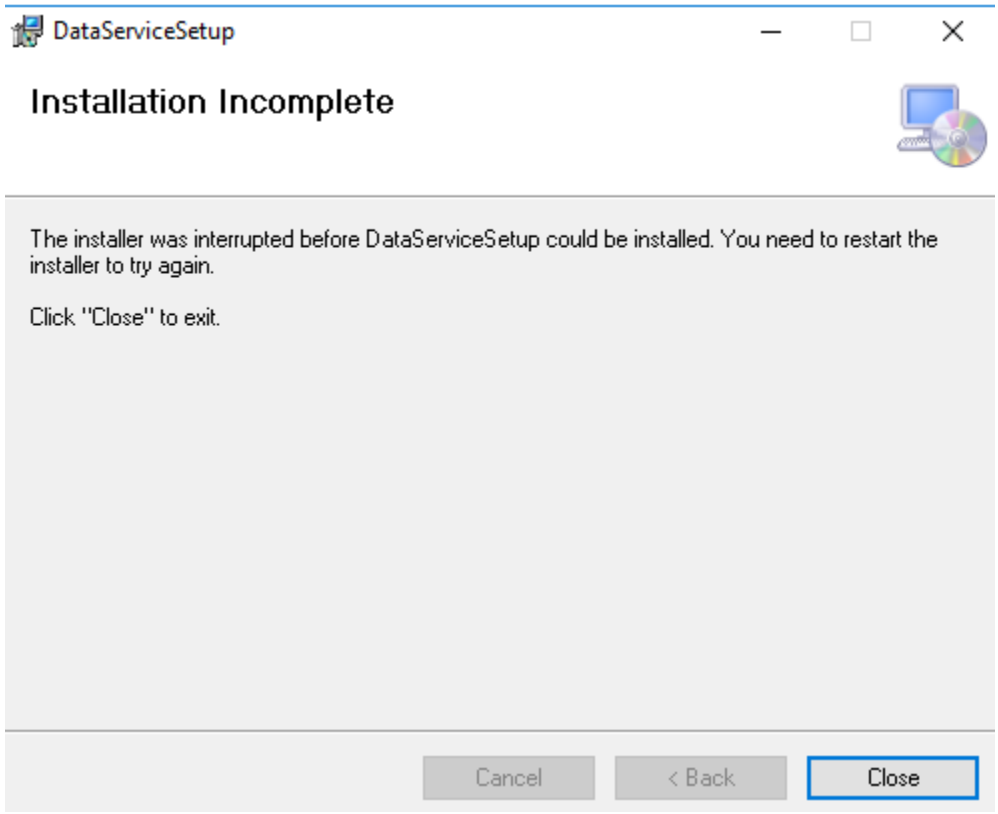
1. Navigate to the **Local Disk (C:)** > **Deploy** > **DataServiceAppSetup** and right-click to **Install.**



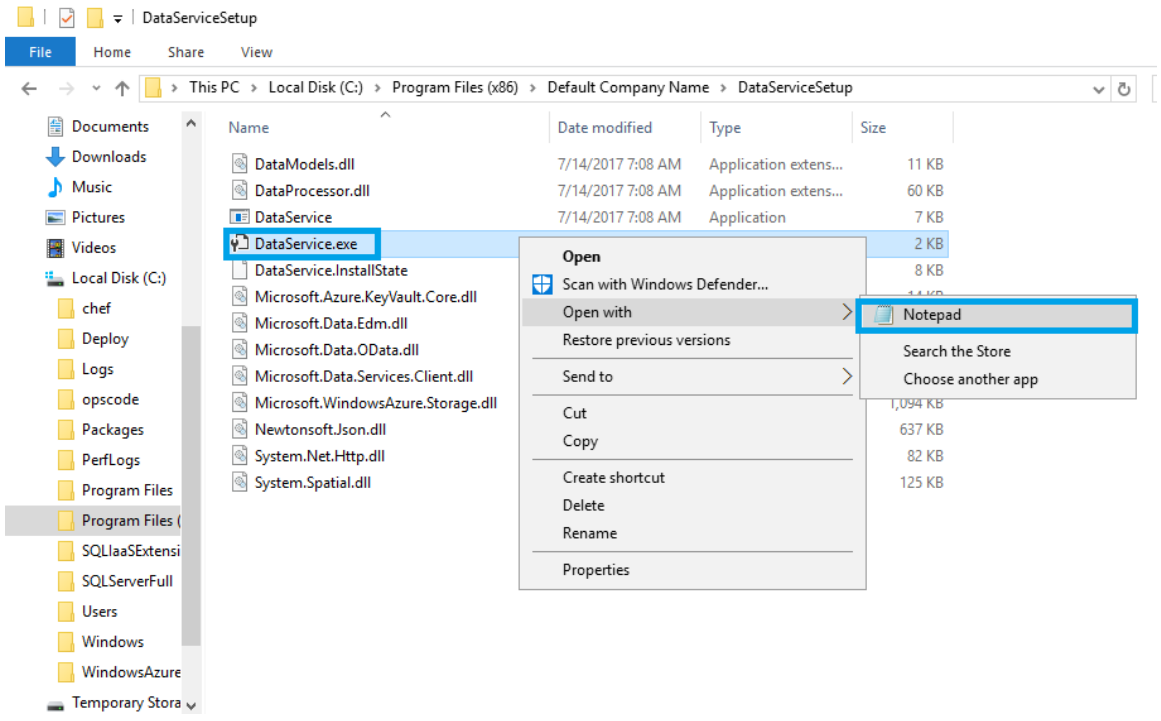
2. Click on **Next**



3. Click on **Close** after the installation complete.

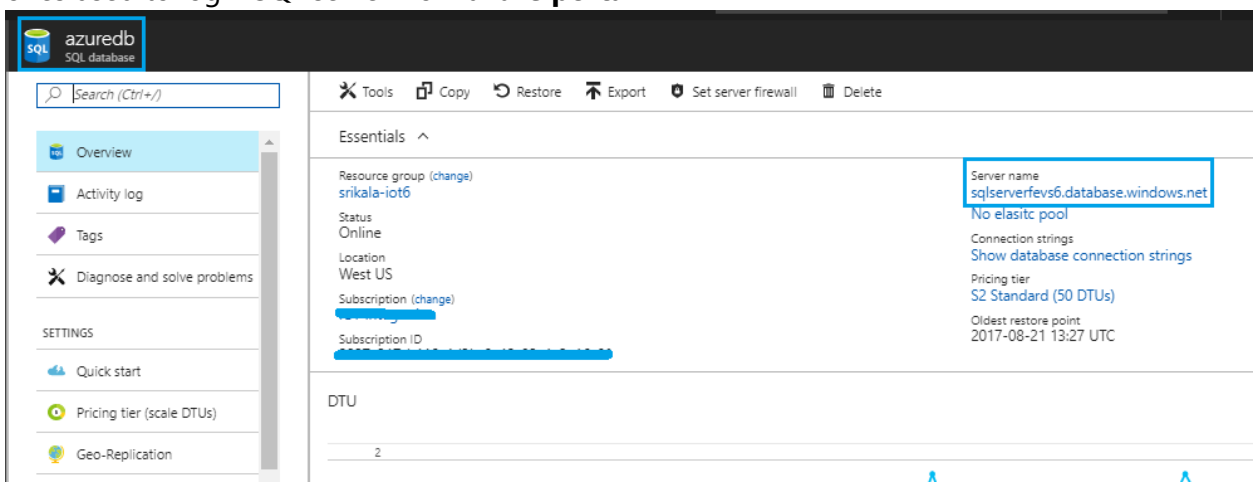


4. Navigate to **Local Disk (C:) > Program Files (*86) > Default company name > Data Services Setup >** Right click on **Dataservice.exe,** then file open with notepad.

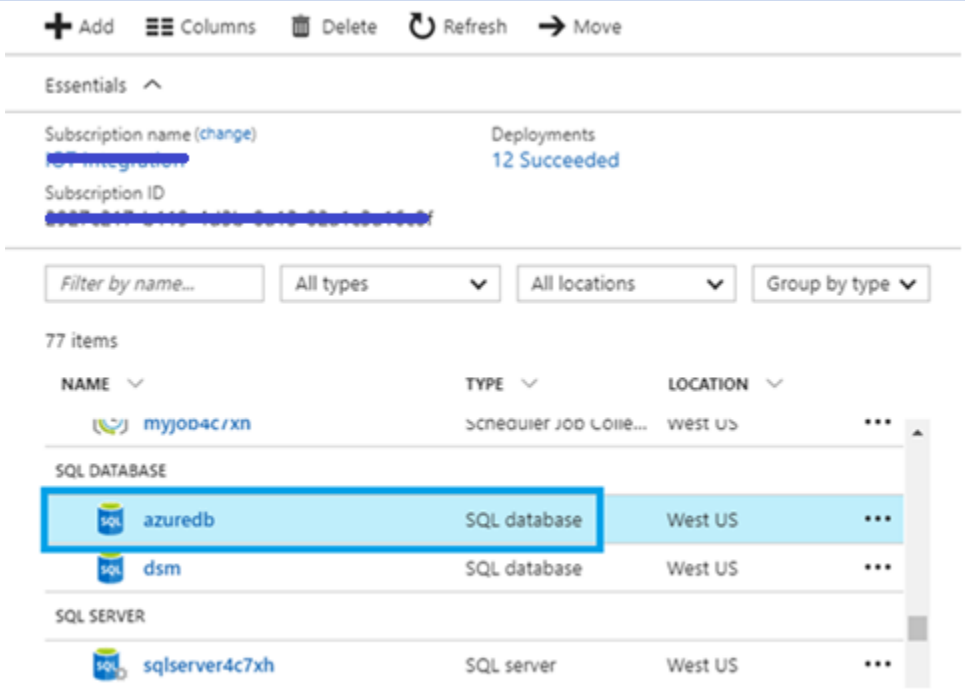


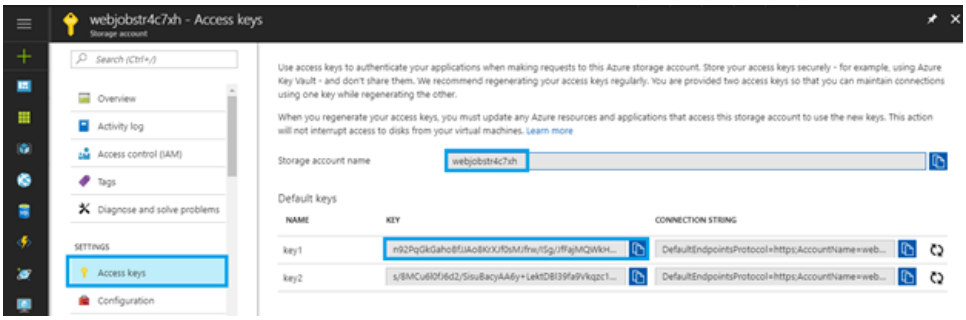
5. Before proceeding, you must update the values in azure connection string, Storage connection string, pi server connection string.

   In **Azure connection string** under **value,** you must take the azure SQL pass environment server name**.** Set **Initial catalog** as azure database name, **user id** and **password** as the ones used to login SQL server from **azure portal**



   Storage Connection String: Here, update the **account name** and **account key values** of **web job storage account** from **azure portal**

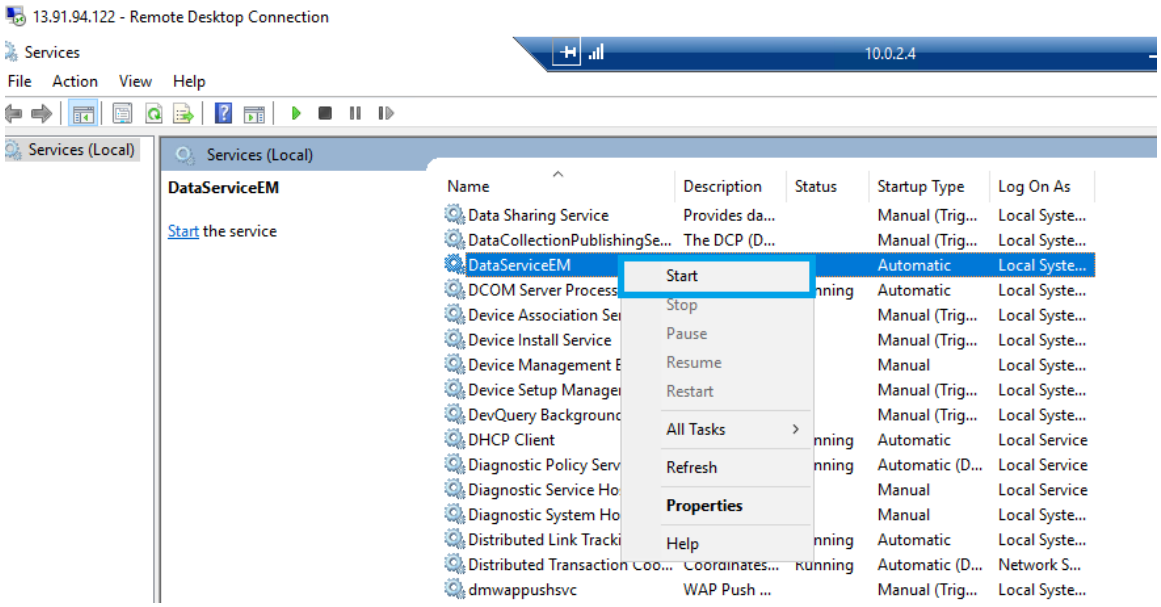




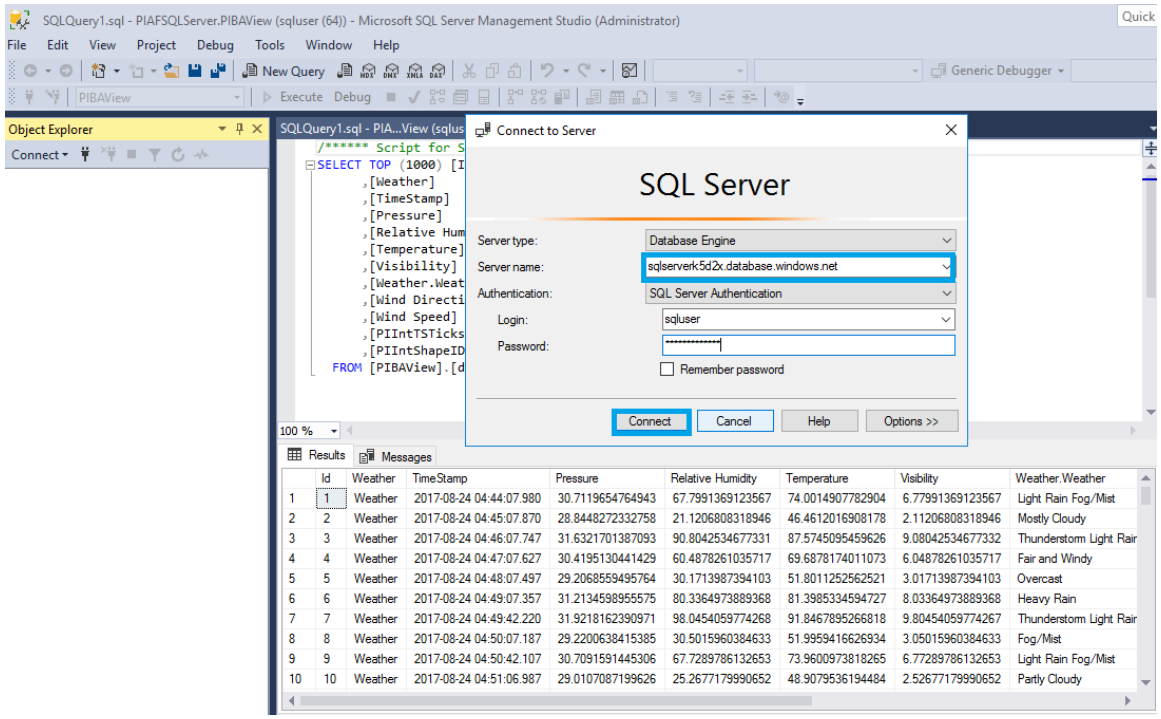
Pi Connection String: Set the **data source** as the AF server name **PIAFSQLServer**, **Initial catalog** as created database name in PIAF server which you created in PI system explorer, and the id/password as the ones used to login the SQLServer Management studio.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <appSettings>
    <add key="PiServer" value="PiServer1" />
    <add key="AzureConnectionString" value="Server=tcp:sqlserver4c7xh.database.windows.net,1433;Initial Catalog=azuredb;Persist Security Info=False;User ID=sqluser;P
    <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=webjobstr4c7xh;AccountKey=n92PqGkGaho8f
    <add key="PiServerConnectionString" value="data source=PIAFSQLServer;initial catalog=PIBAView;persist security info=True;user id=sqluser;password=Password@1234"
  </appSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>
```

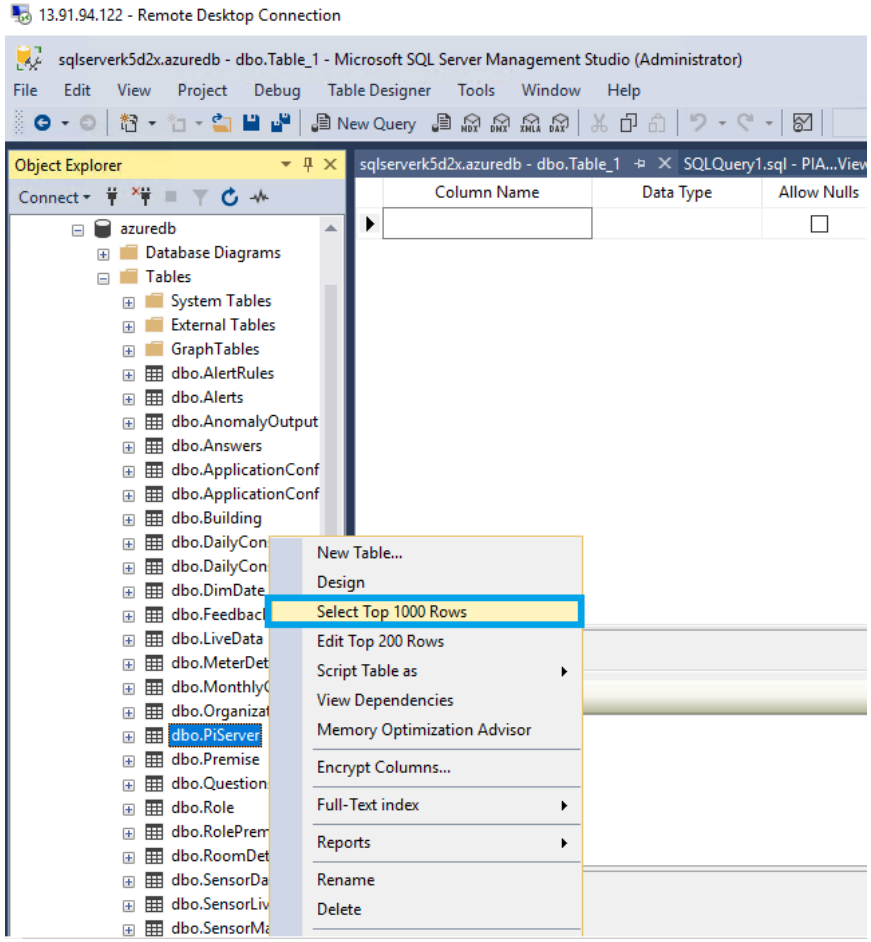
6. After updating the values in the data service.exe files, navigate **Start > Service** to start the DataServicesEM.



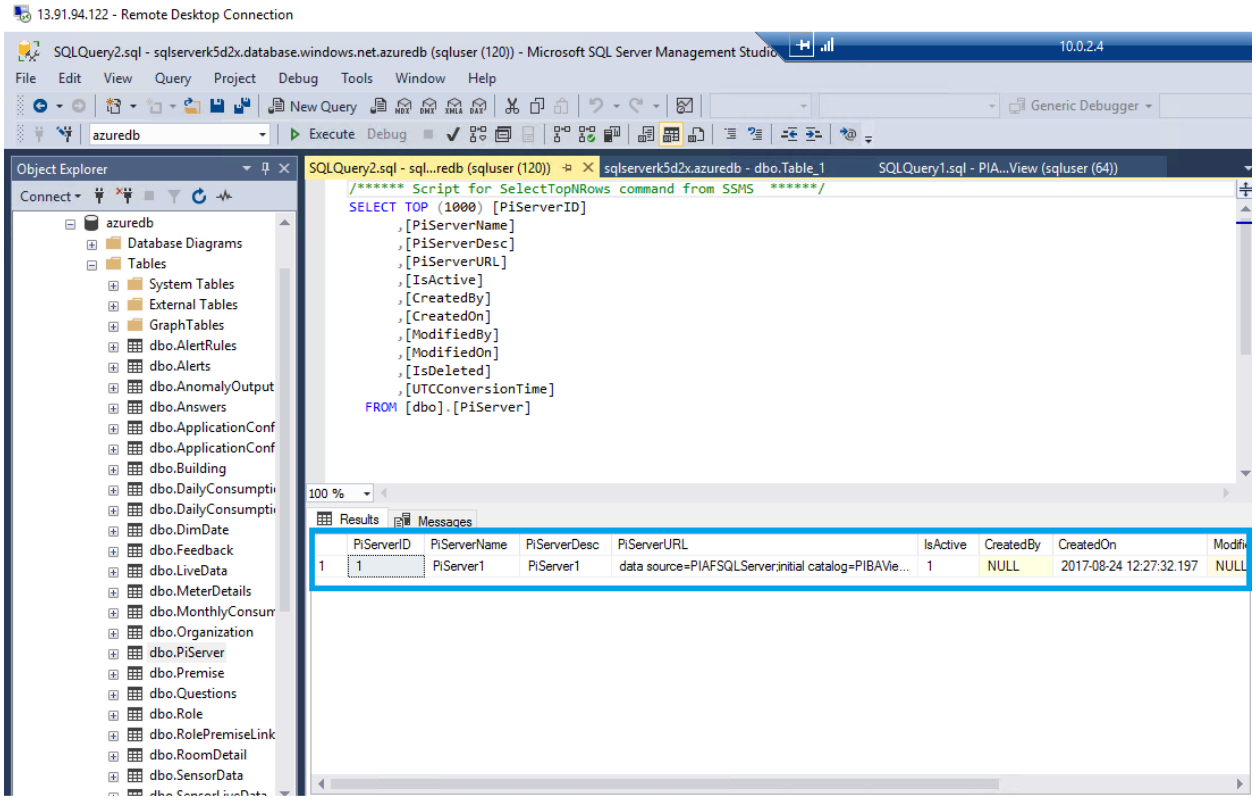
7. To check the data, we need to login to SQL server management studio in AF server with azure SQL server name with SQL login credentials and click on **connect.**

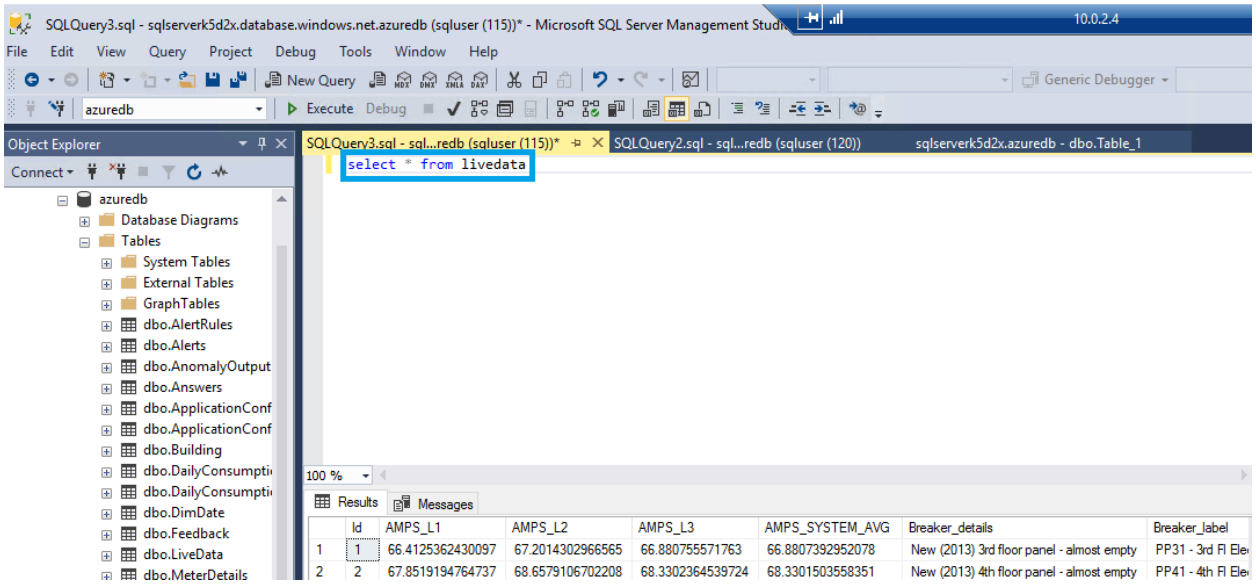


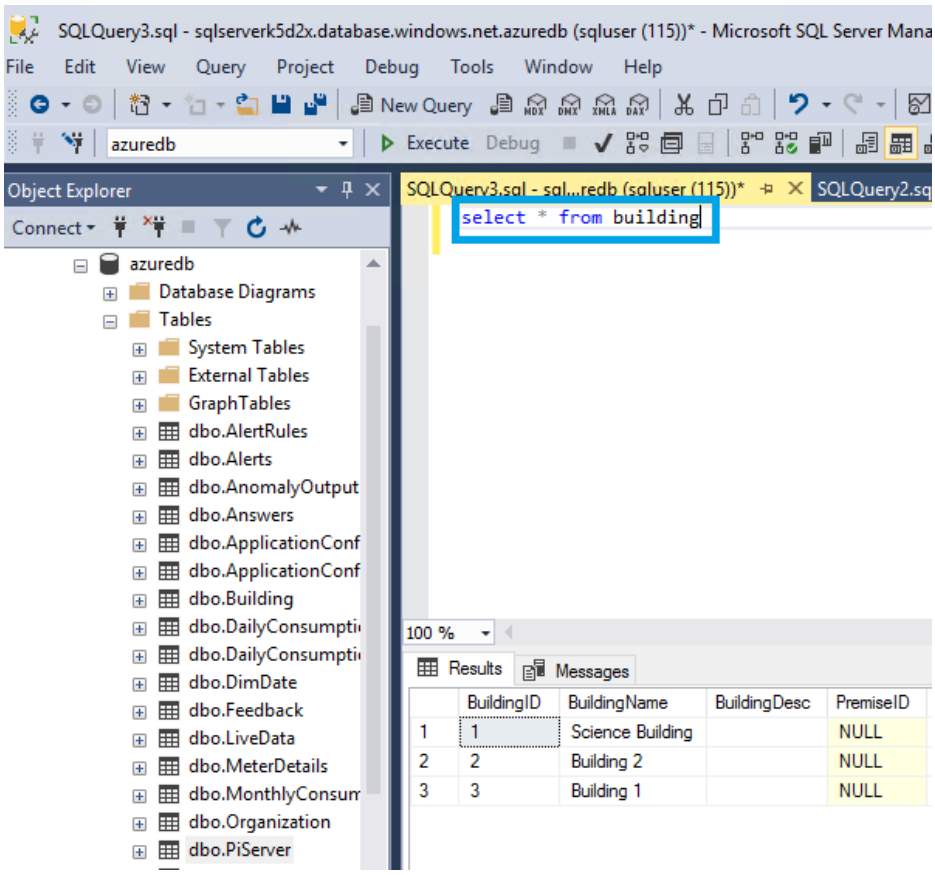
8. Navigate to **azuredb** > **tables** > right-click on **PiServer** data > select **Top 1000 Rows.**

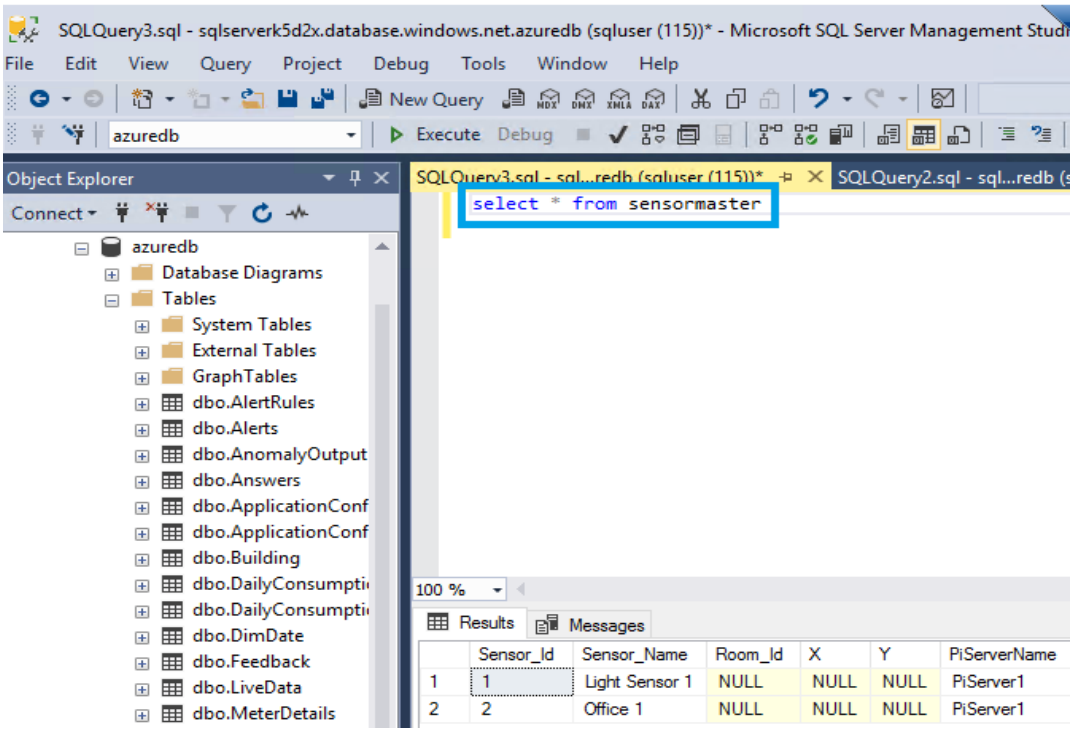


9. Check the updated table.

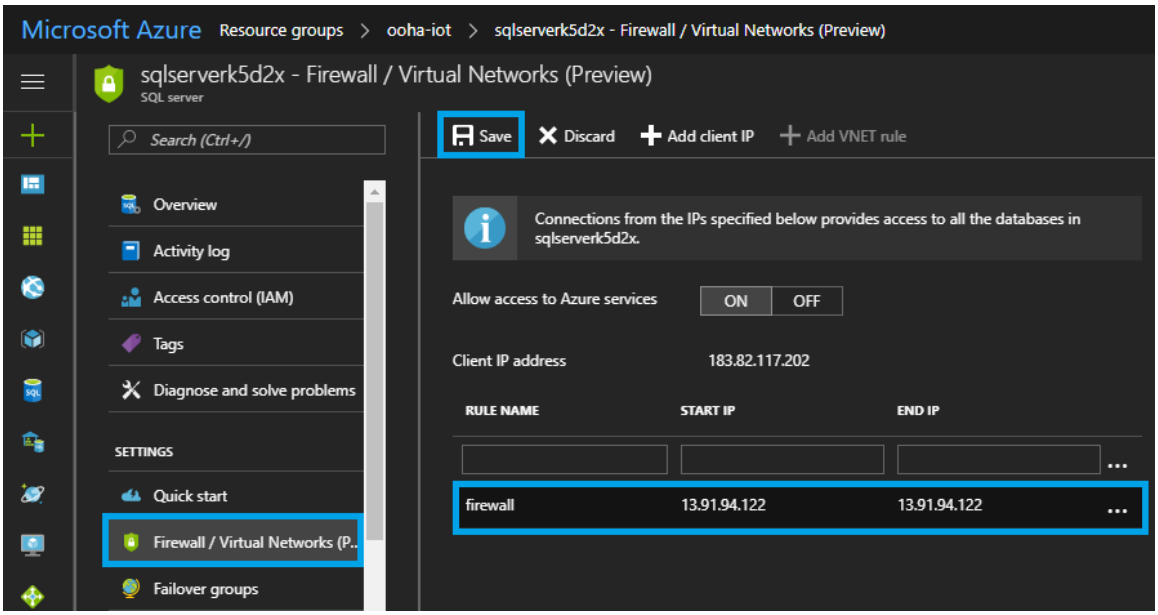




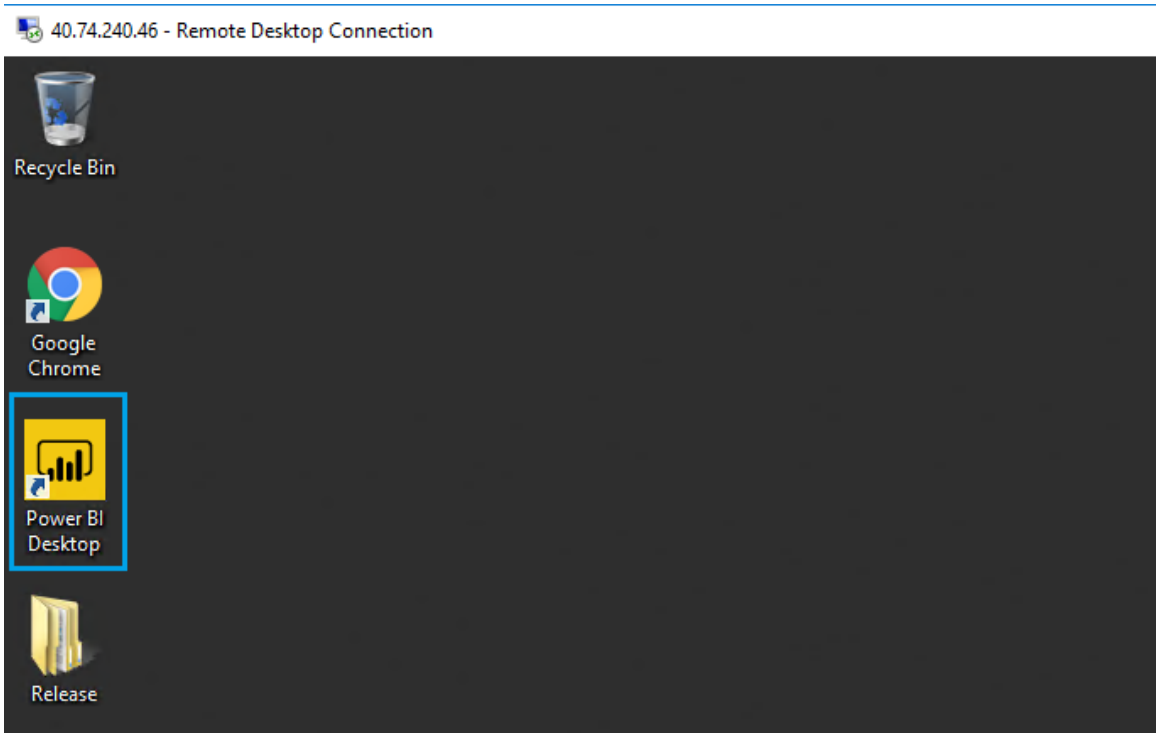

SQLQuery3.sql - sqlserverk5d2x.database.windows.net.azuredb (sqluser (115))* - Microsoft SQL Server Mana
File Edit View Query Project Debug Tools Window Help
New Query
azuredb
Execute Debug
Object Explorer
Connect
azuredb
Database Diagrams
Tables
System Tables
External Tables
GraphTables
dbo.AlertRules
dbo.Alerts
dbo.AnomalyOutput
dbo.Answers
dbo.ApplicationConf
dbo.ApplicationConf
dbo.Building
dbo.DailyConsumpti
dbo.DailyConsumpti
dbo.DimDate
dbo.Feedback
dbo.LiveData
dbo.MeterDetails
dbo.MonthlyConsum
dbo.Organization
dbo.PiServer
SQLQuery3.sql - sql...redb (sqluser (115))*
SQLQuery2.sq
select * from building
100 %
Results
Messages
BuildingID BuildingName BuildingDesc PremiseID
1 1 Science Building NULL
2 2 Building 2 NULL
3 3 Building 1 NULL


SQLQuery3.sql - sqlserverk5d2x.database.windows.net.azuredb (sqluser (115))* - Microsoft SQL Server Management Studi
File Edit View Query Project Debug Tools Window Help
New Query
azuredb
Execute Debug
Object Explorer
Connect
azuredb
Database Diagrams
Tables
System Tables
External Tables
GraphTables
dbo.AlertRules
dbo.Alerts
dbo.AnomalyOutput
dbo.Answers
dbo.ApplicationConf
dbo.ApplicationConf
dbo.Building
dbo.DailyConsumpti
dbo.DailyConsumpti
dbo.DimDate
dbo.Feedback
dbo.LiveData
dbo.MeterDetails
SQLQuery3.sql - sql...redb (sqluser (115))*
SQLQuery2.sql - sql...redb
select * from sensormaster
100 %
Results
Messages
Sensor_Id Sensor_Name Room_Id X Y PiServerName
1 1 Light Sensor 1 NULL NULL NULL PiServer1
2 2 Office 1 NULL NULL NULL PiServer1

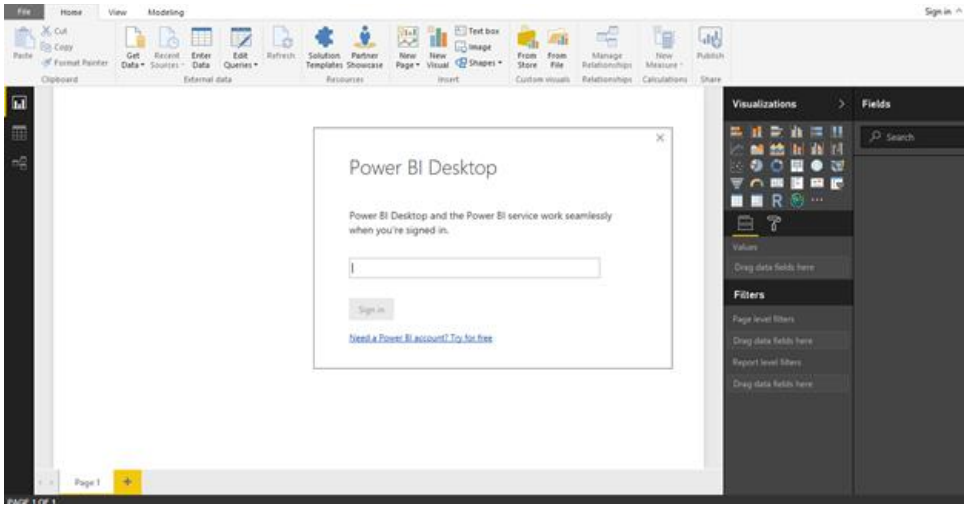
10. Update the firewall settings by adding the Bastion server IP. Navigate to **Azure Paas environment** > click on **firewall/virtual networks** > provide the **Public IP of Bastion server** and **Save** changes.

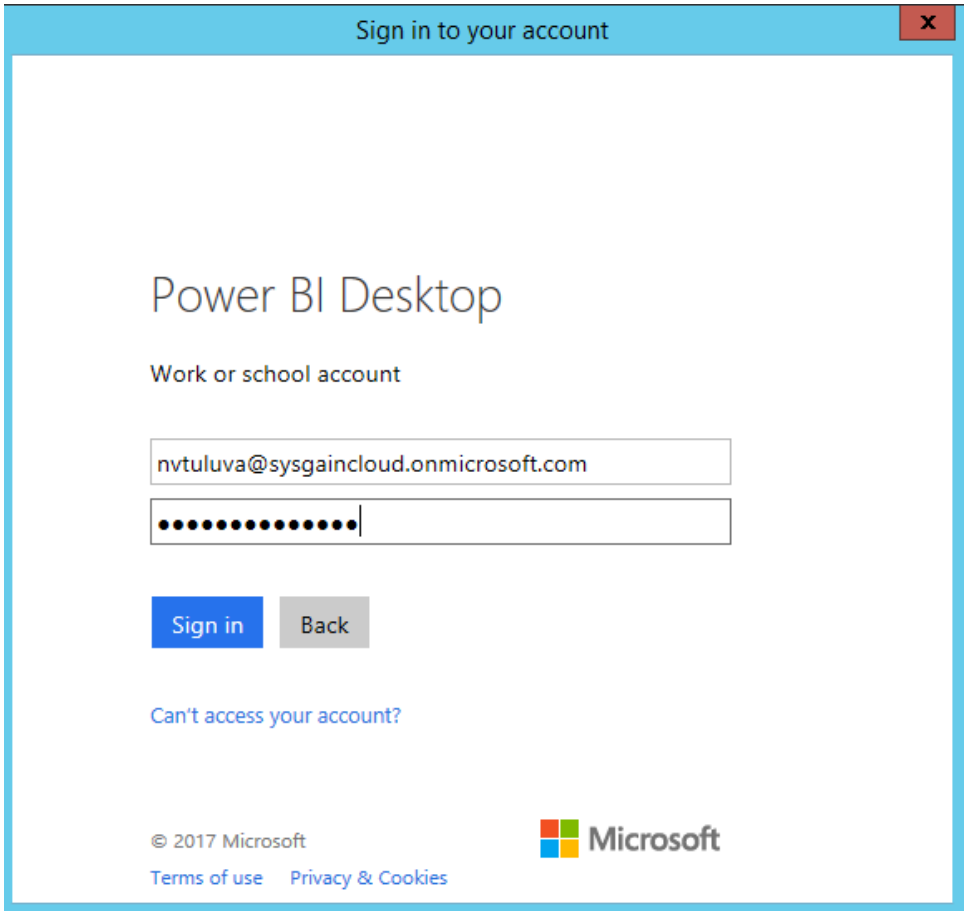


11. Login to the Bastionserver you can see the power BI desktop in Bastionserver desktop, Click on that Power BI desktop.

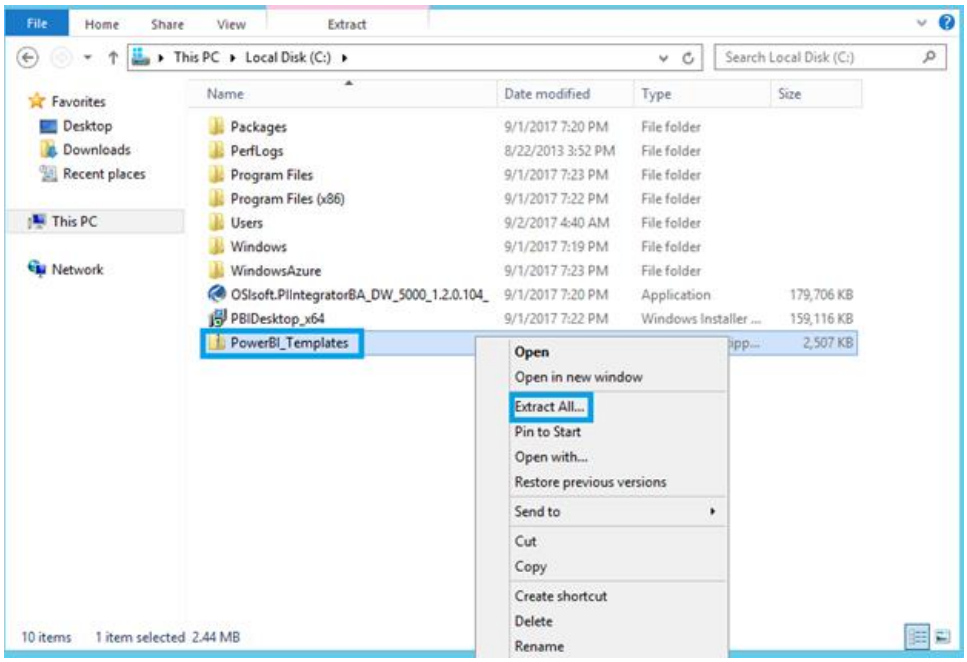


12. Log in with the same credentials used while registration of webapp with power BI you don't need to create a power BI account.

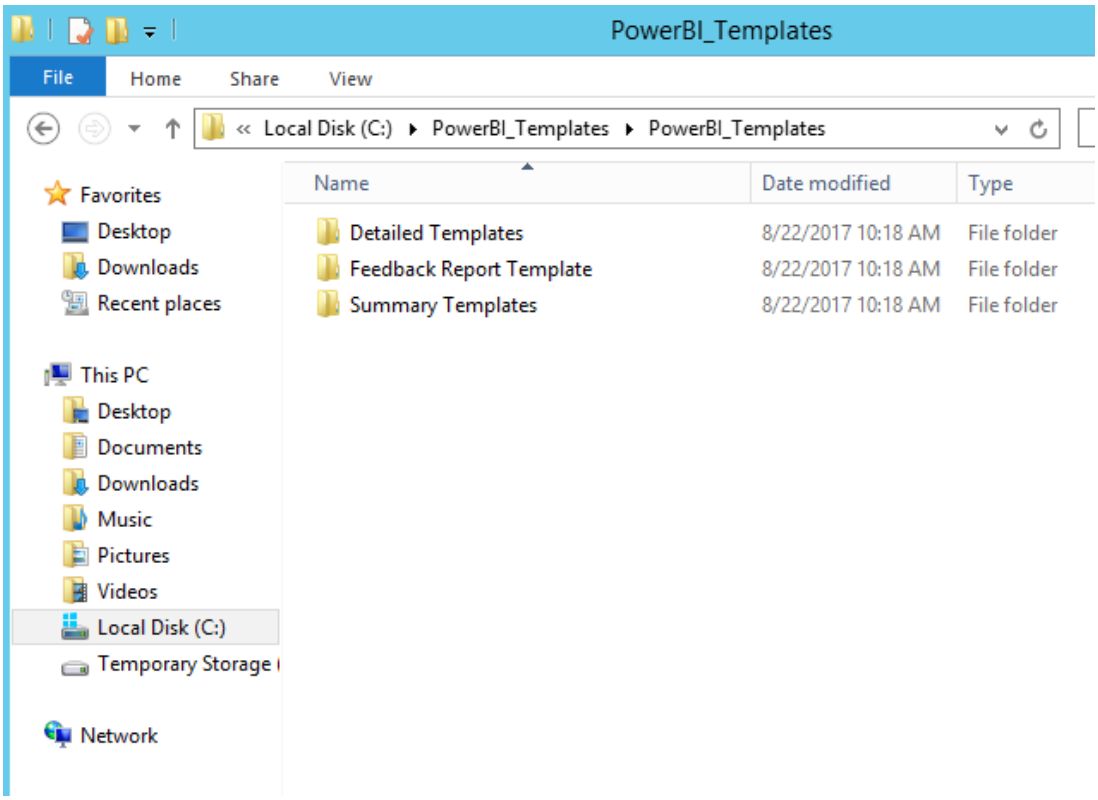




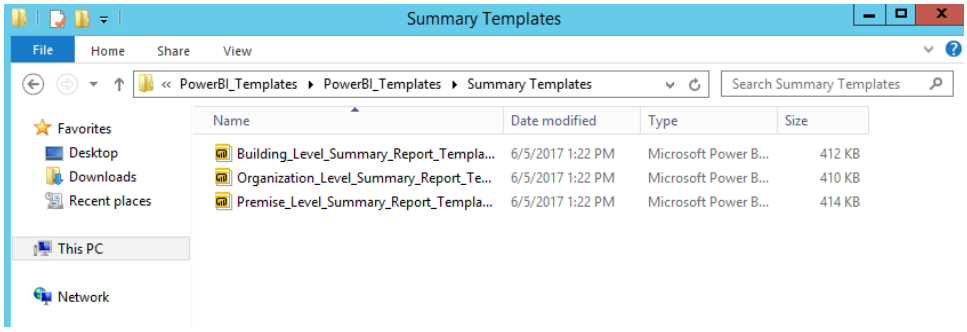
13. In Bastion server, navigate to **Local disk (C:)** > **unzip the Power Bi templates** > **Power Bi templates**.



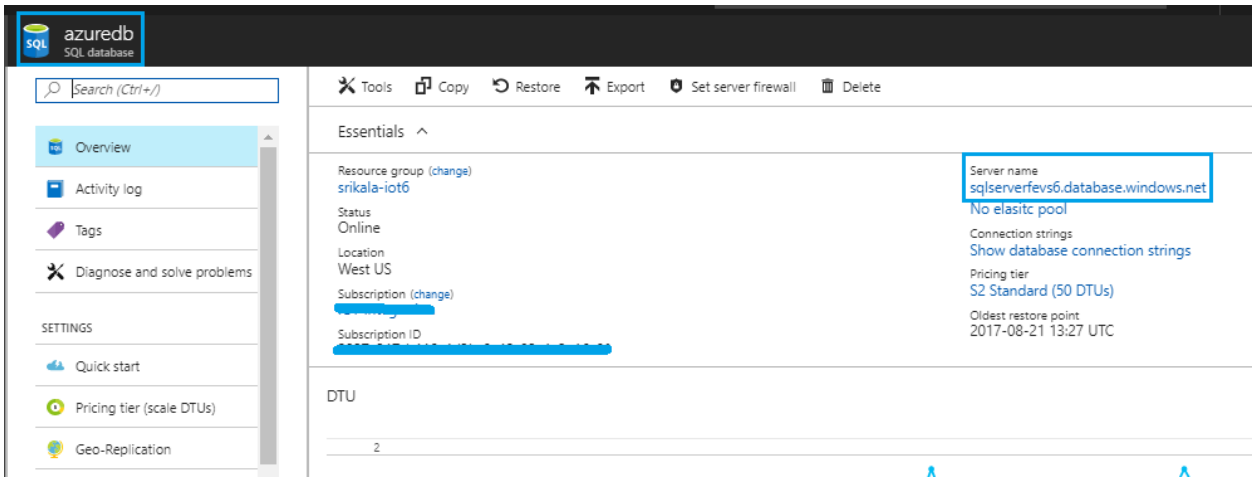
14. You can view Power BI templates in the Local disk (C:)

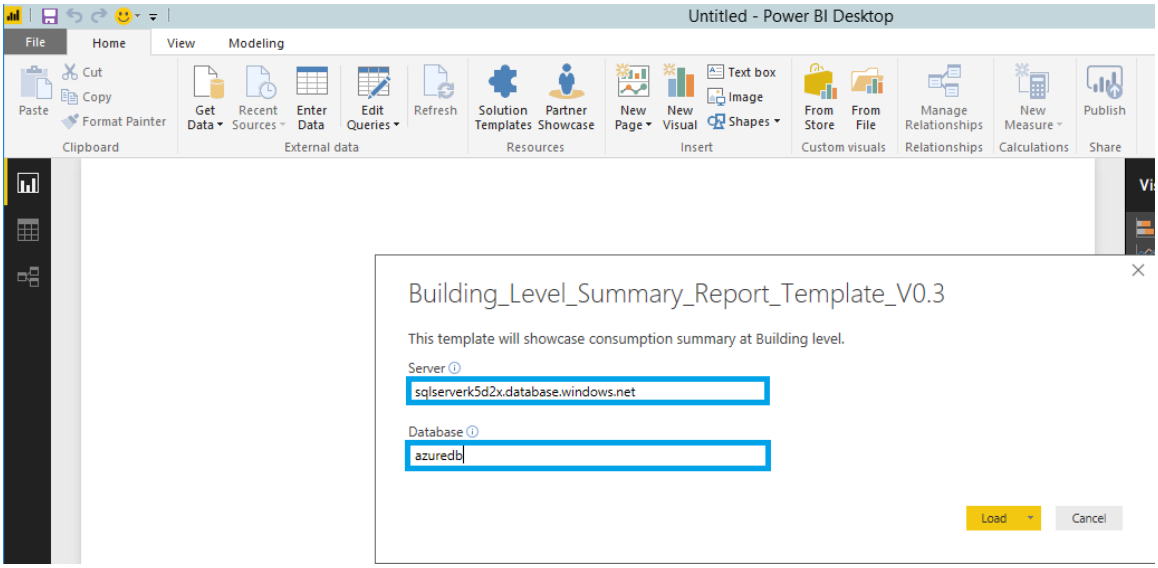


15. Navigate to the summary templates folder, click on "**Building_level_summary templates**" click on keep using Microsoft Power BI Desktop

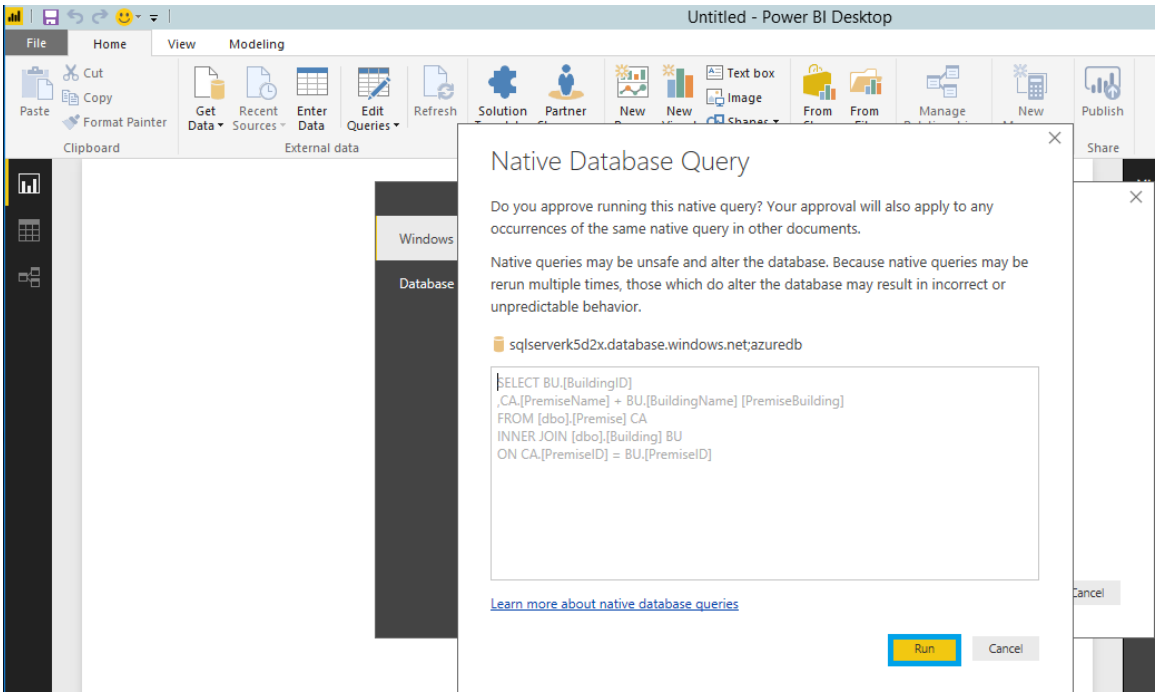


16. It prompts for power BI server and database details, provide you're Azure SQL server name and azure SQL database name from your deployed azure SQLServer .and click on **Load**.

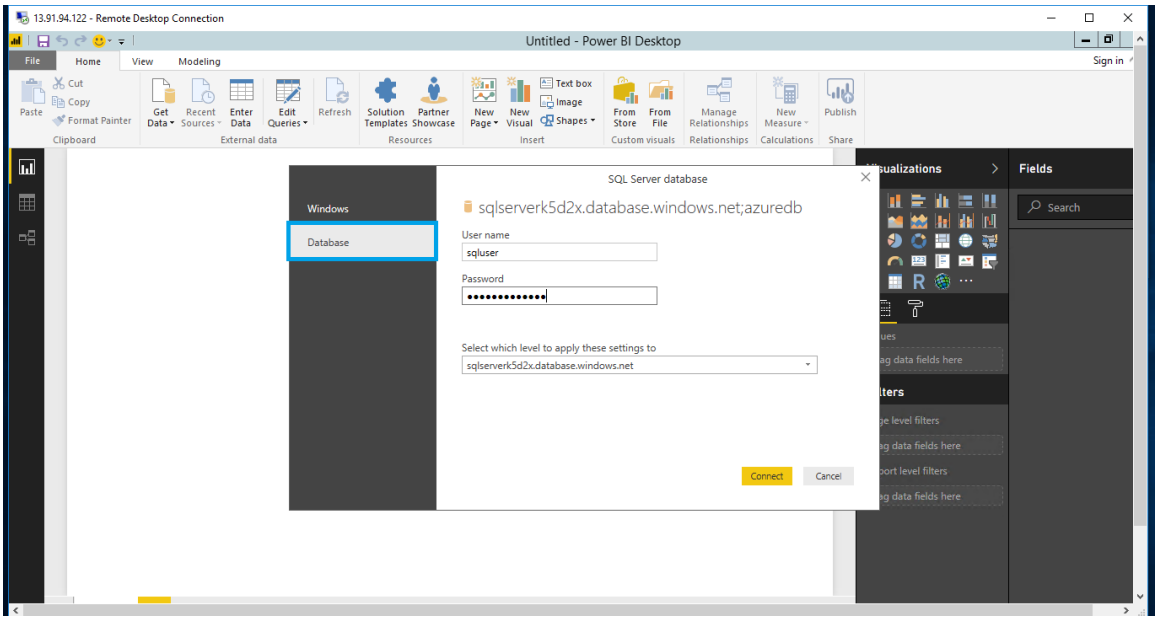

azuredb
SQL database
Search (Ctrl+/)
Overview
Activity log
Tags
Diagnose and solve problems
SETTINGS
Quick start
Pricing tier (scale DTUs)
Geo-Replication
Tools
Copy
Restore
Export
Set server firewall
Delete
Essentials
Resource group (change)
srikala-iot6
Status
Online
Location
West US
Subscription (change)
Subscription ID
Server name
sqlserverfevs6.database.windows.net
No elasitc pool
Connection strings
Show database connection strings
Pricing tier
S2 Standard (50 DTUs)
Oldest restore point
2017-08-21 13:27 UTC
DTU
2


Untitled - Power BI Desktop
File
Home
View
Modeling
Paste
Cut
Copy
Format Painter
Clipboard
Get Data
Recent Sources
Enter Data
Edit Queries
Refresh
External data
Solution Templates
Partner Showcase
Resources
New Page
New Visual
Text box
Image
Shapes
Insert
From Store
From File
Custom visuals
Manage Relationships
Relationships
New Measure
Calculations
Publish
Share
Building_Level_Summary_Report_Template_V0.3
This template will showcase consumption summary at Building level.
Server
sqlserverk5d2x.database.windows.net
Database
azuredb
Load
Cancel

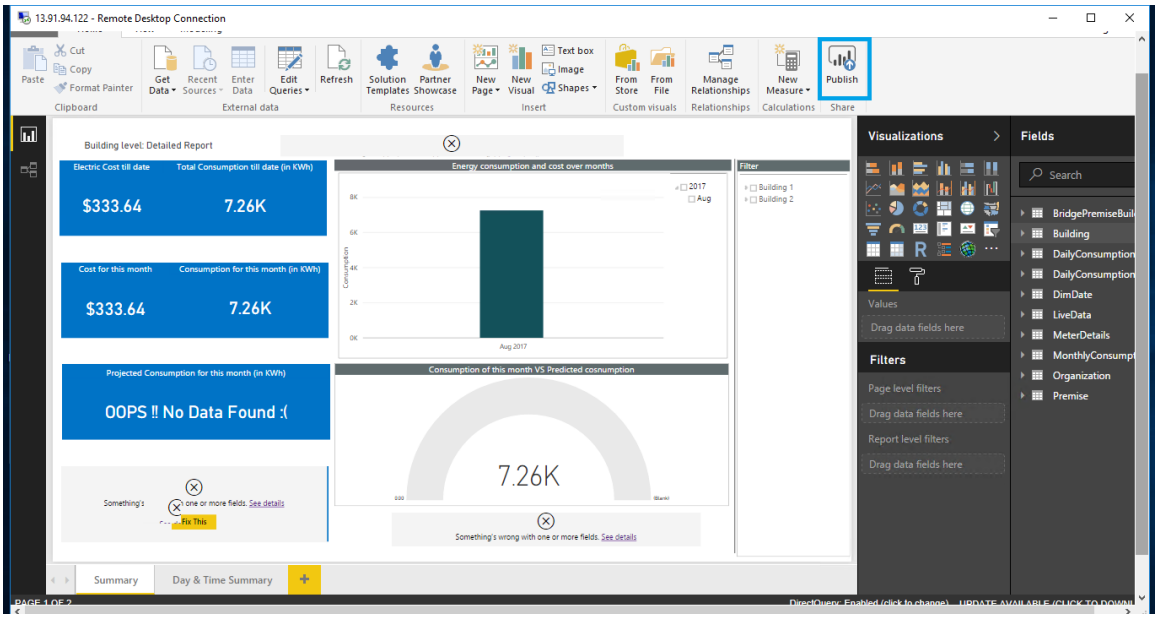
17. Once you click on Load, the "Native Database Query" will appear, click on **Run.**



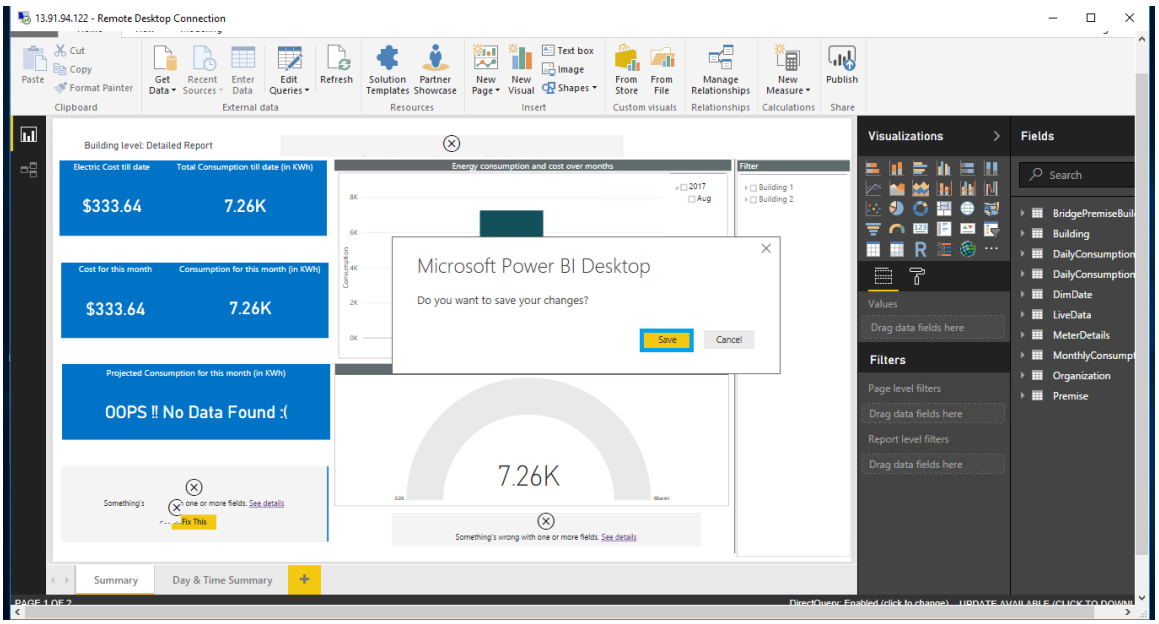
18. Select **Database** after connecting to the Azure SQL Server. Enter the login credentials of Azure database and click on **Connect**.



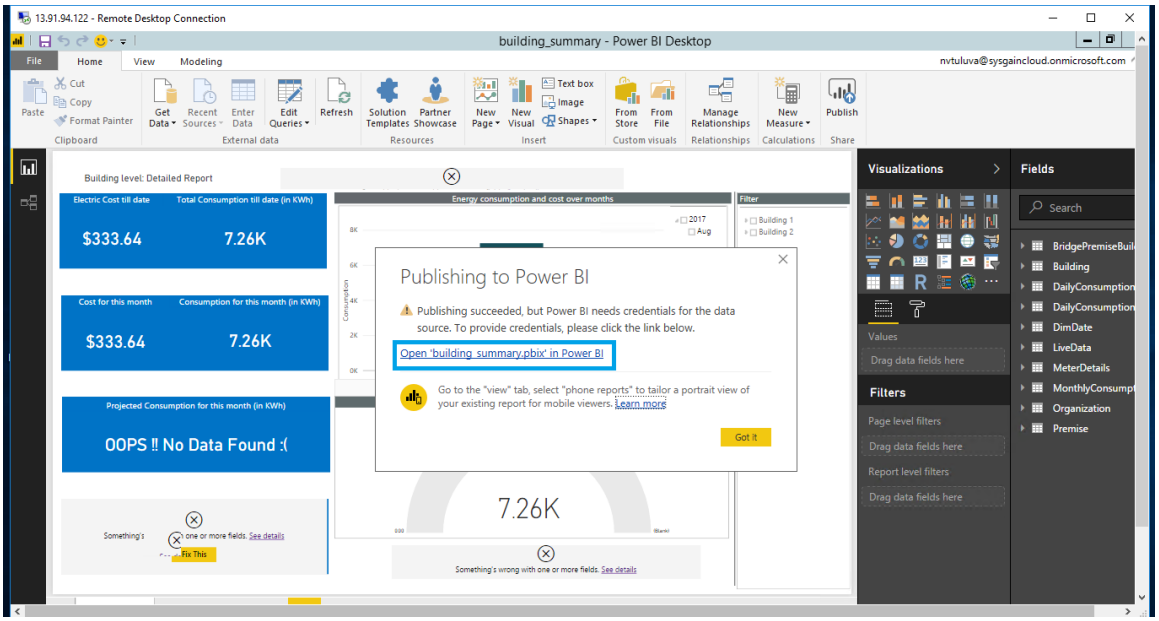
19. Click on **Publish.**



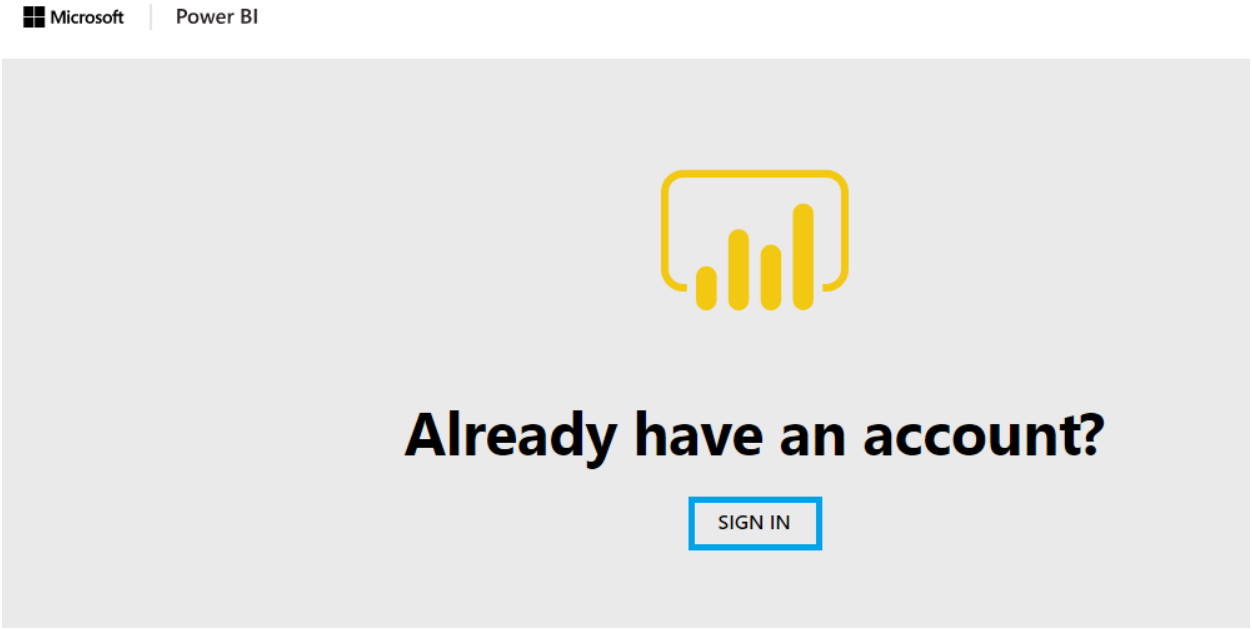
20. **Save** the changes.



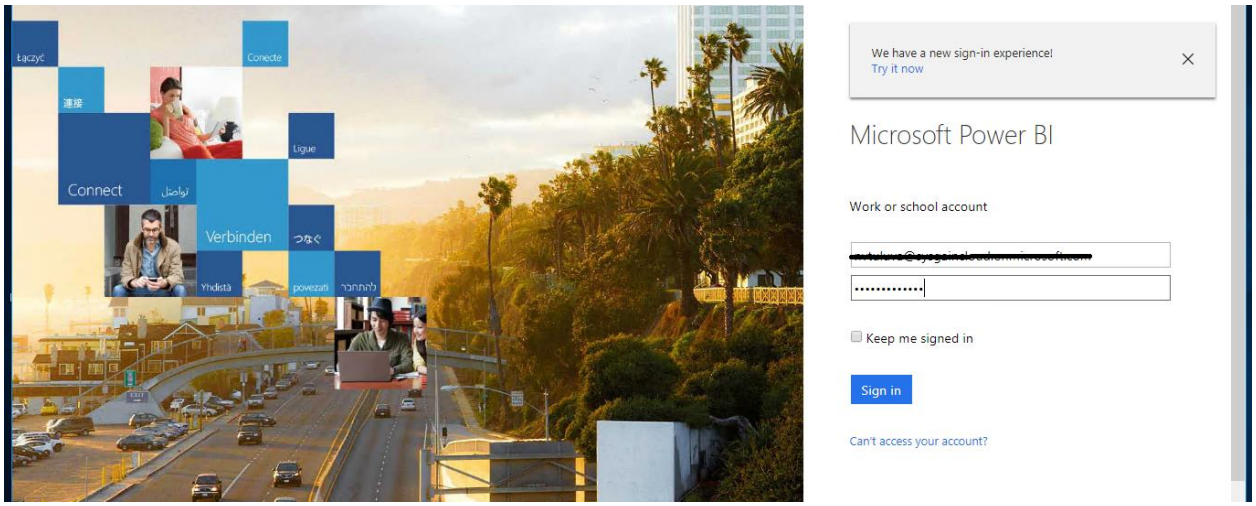
21. Click on the link as shown below, it will open in a web browser.



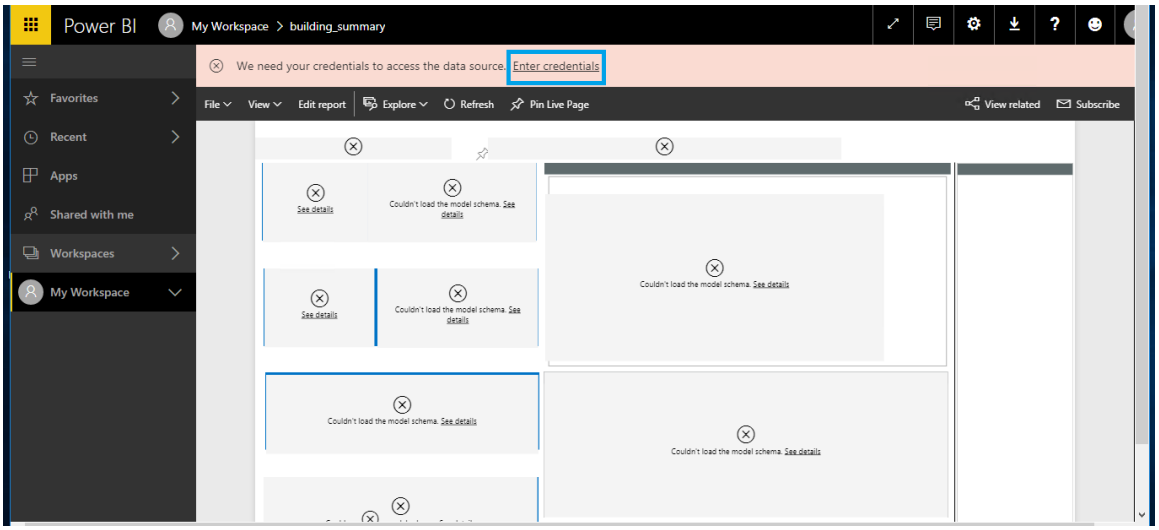
22. Sign in with the same credentials which were used to log to Power BI.



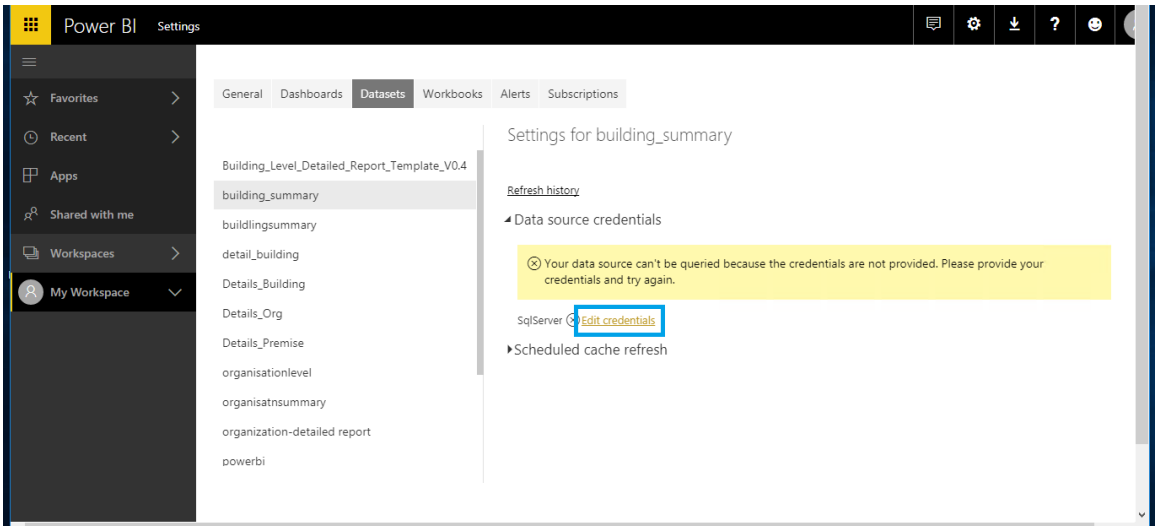
23. Enter the Power BI Credentials.



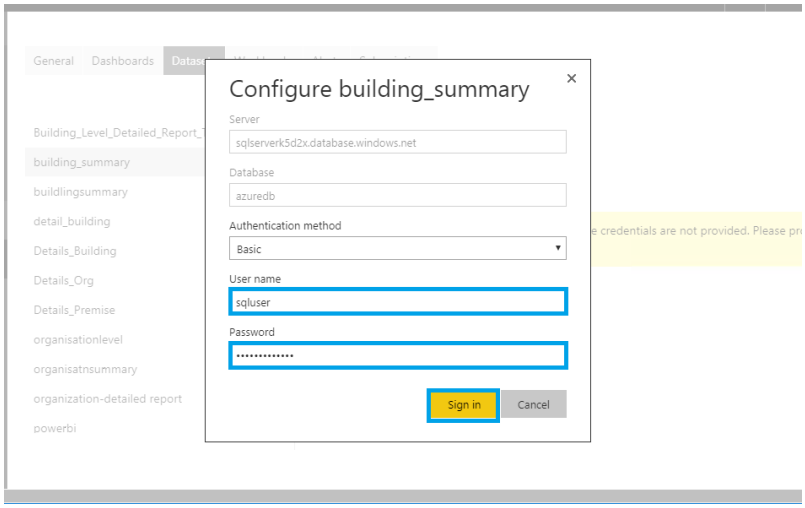
24. Click on **Enter credentials**.



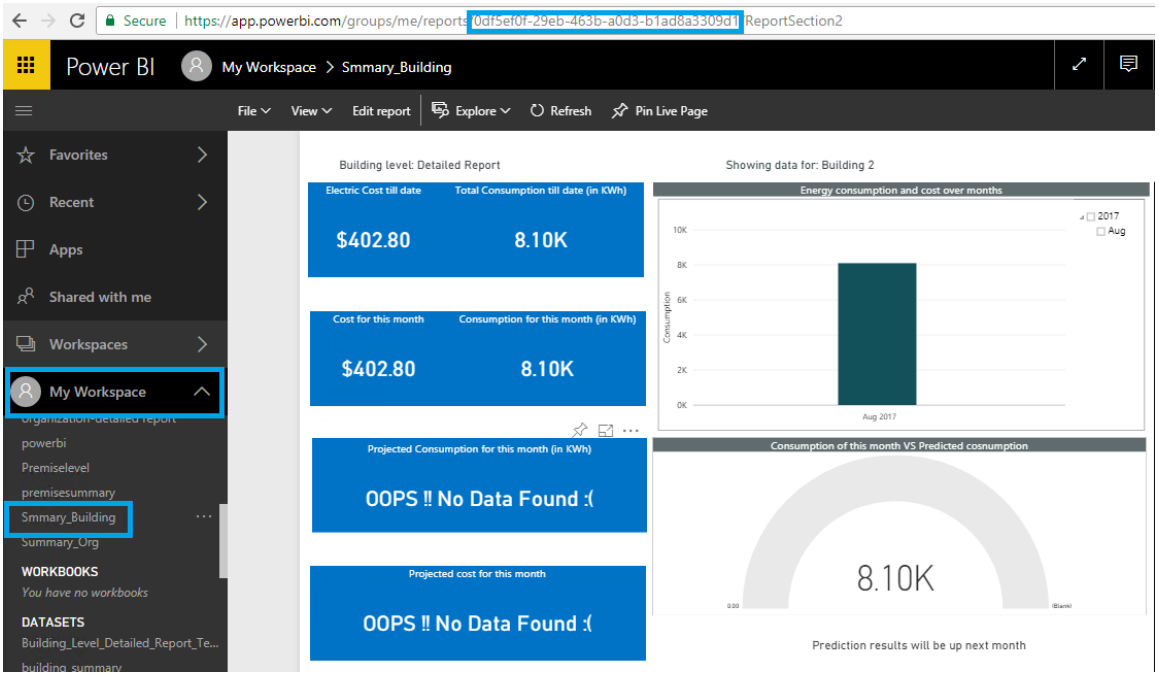
25. Click on **Edit credentials**.



26. Enter the Azure SQL Server **User name** and **Password,** then click **Sign in.**

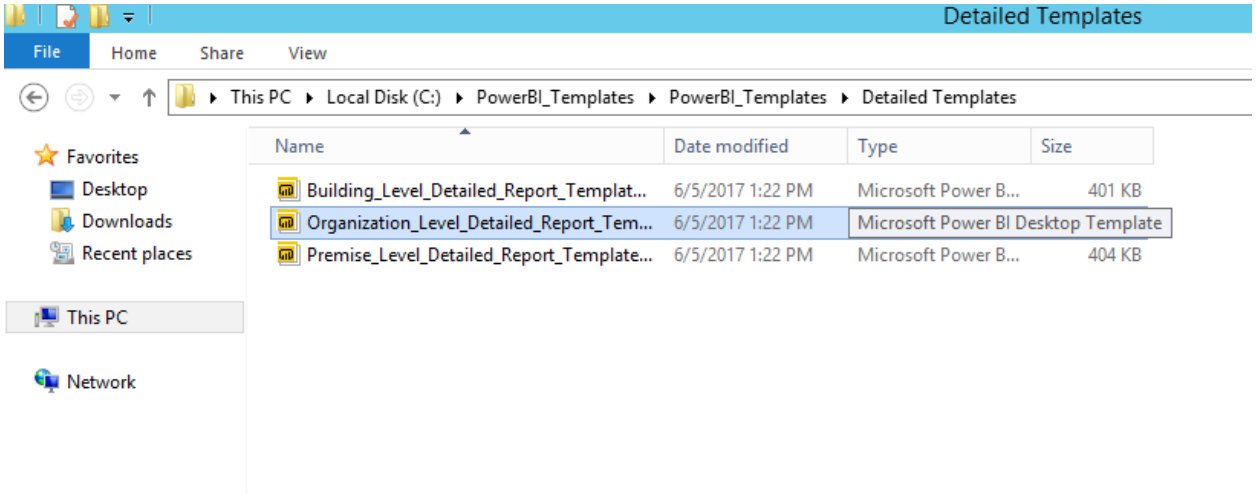


27. **Copy the token** from the URL publishing each template and **save it** for further configuration in web app.

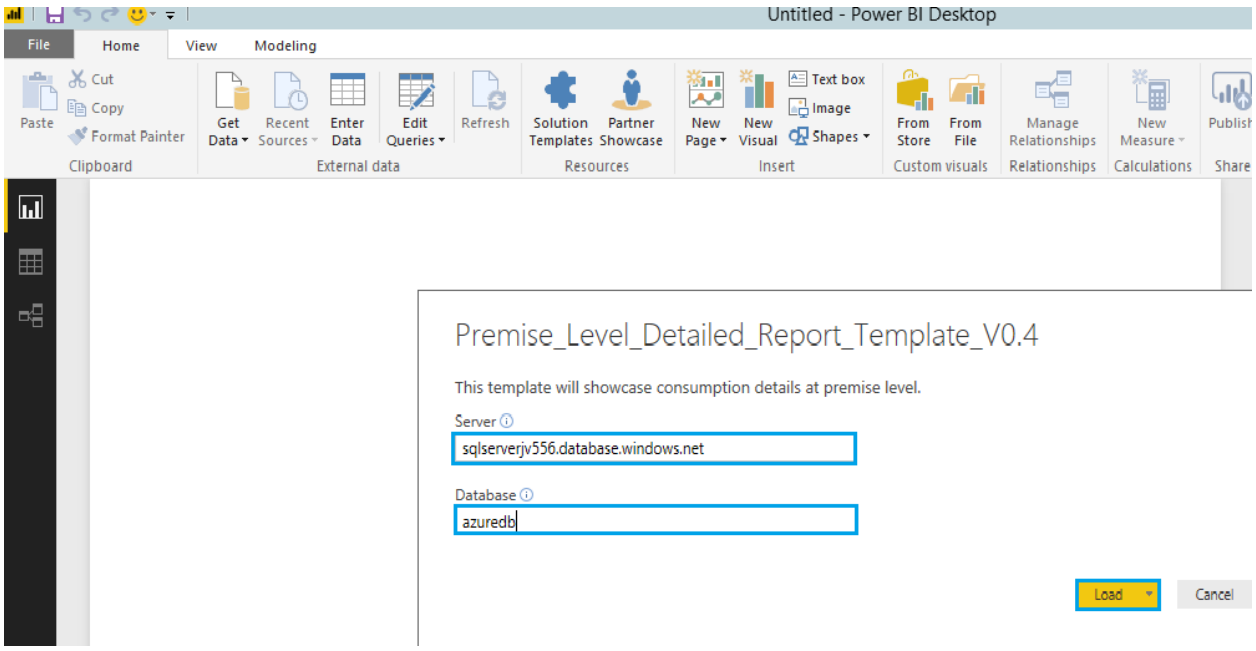


28. Similarly, follow the same process for Organisation and Premise Summary templates.

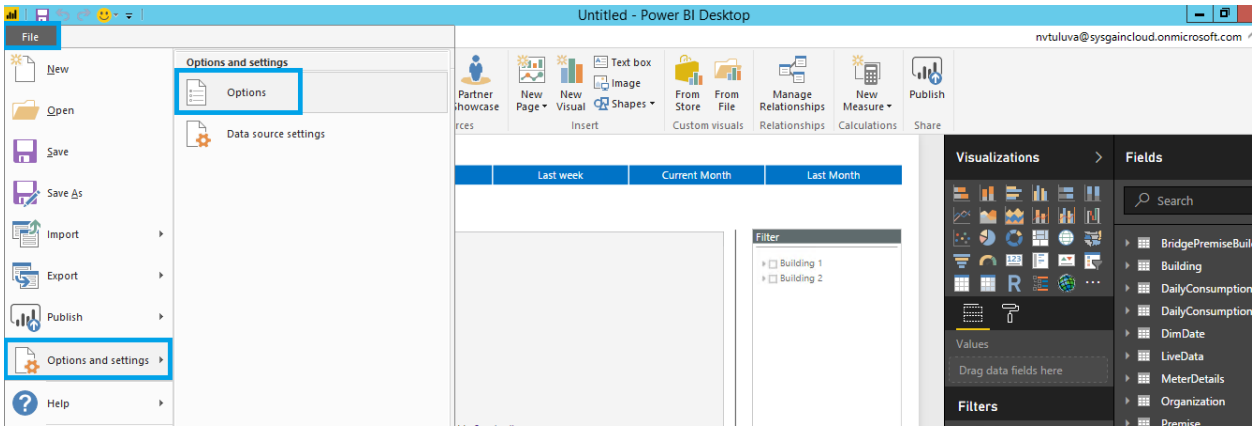
29. Navigate to **Power BI** templates and select **Detailed Template**



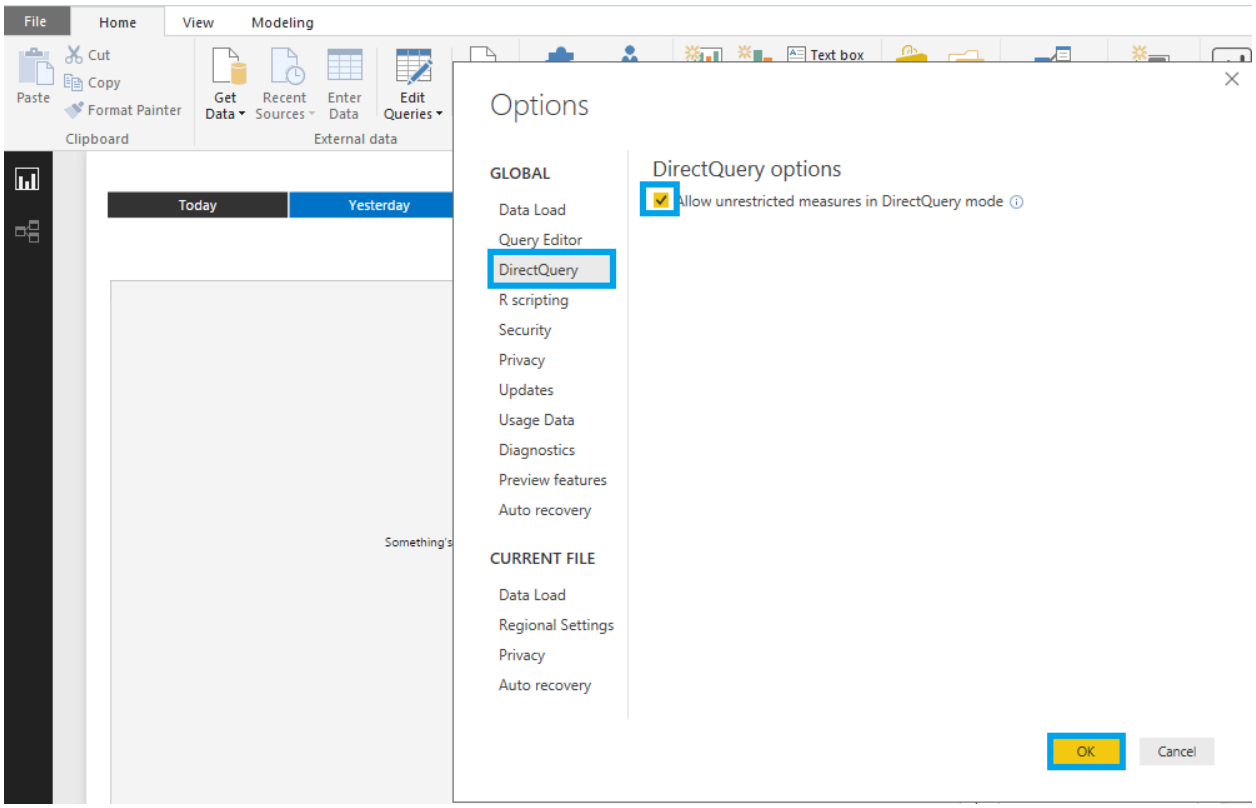
30. Enter the Azure SQL Server name with its password.



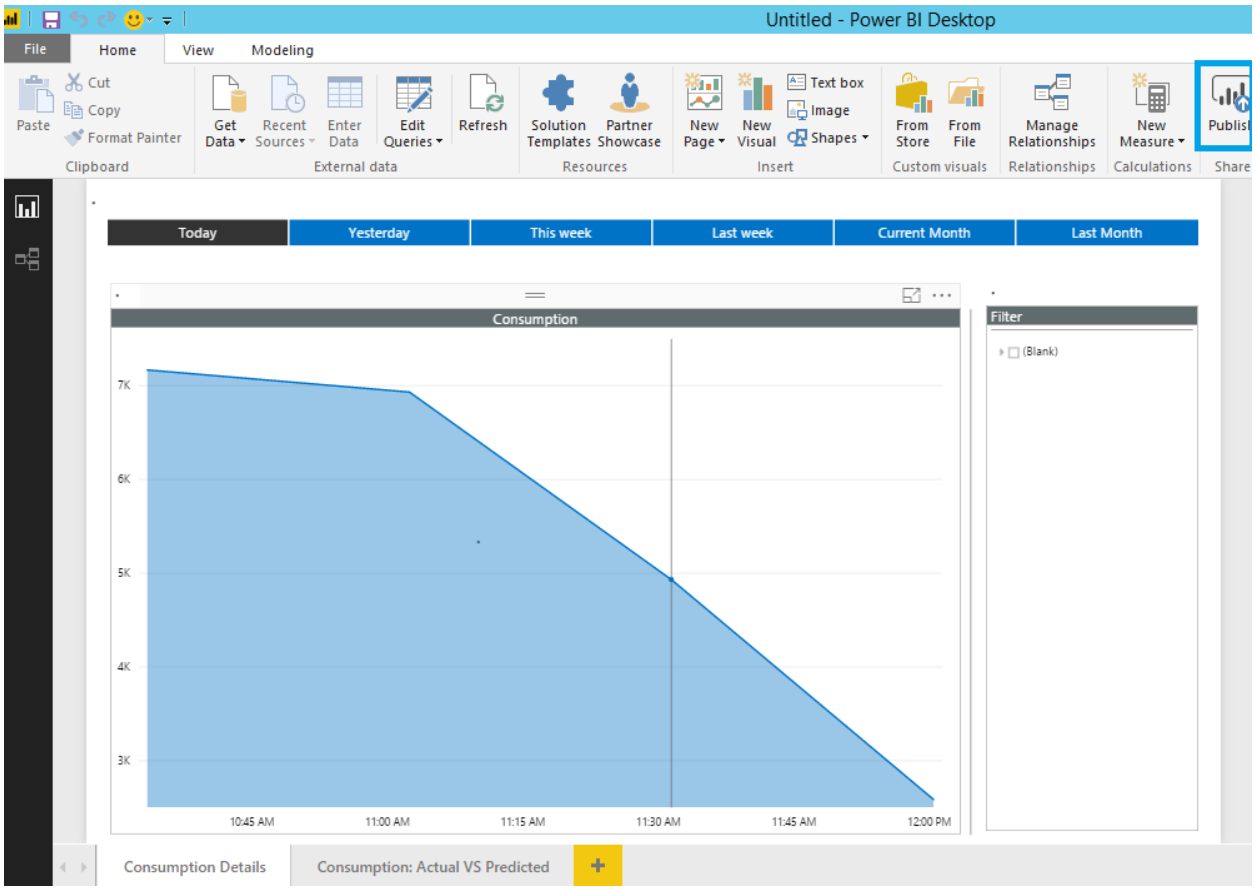
31. Navigate to **File** > **Options and Settings** > **Options**.



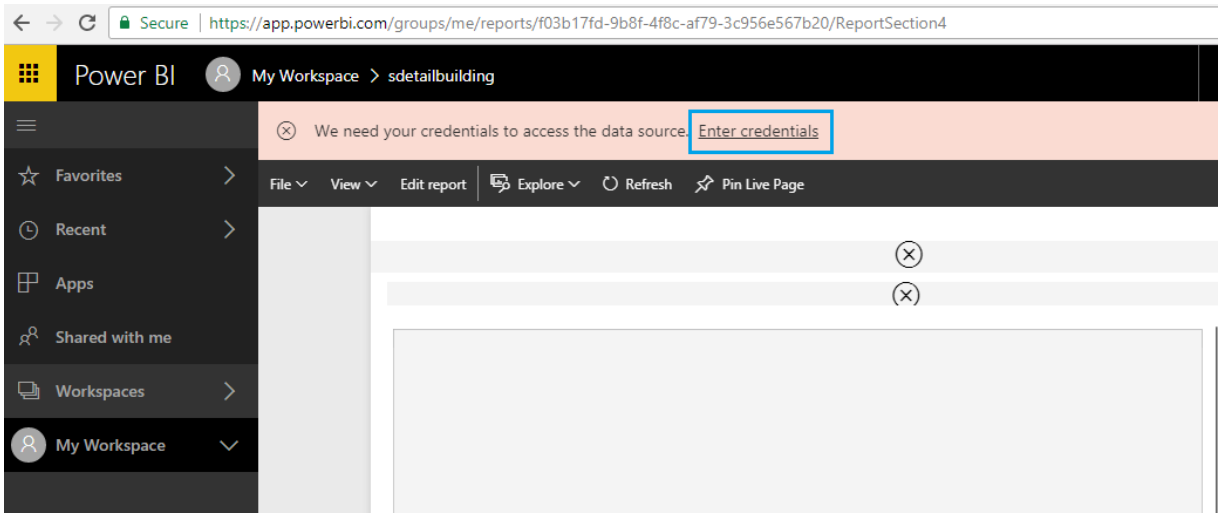
32. Select **DirectQuery** and then click on **OK**. Follow the same Process as done for the Summary template.



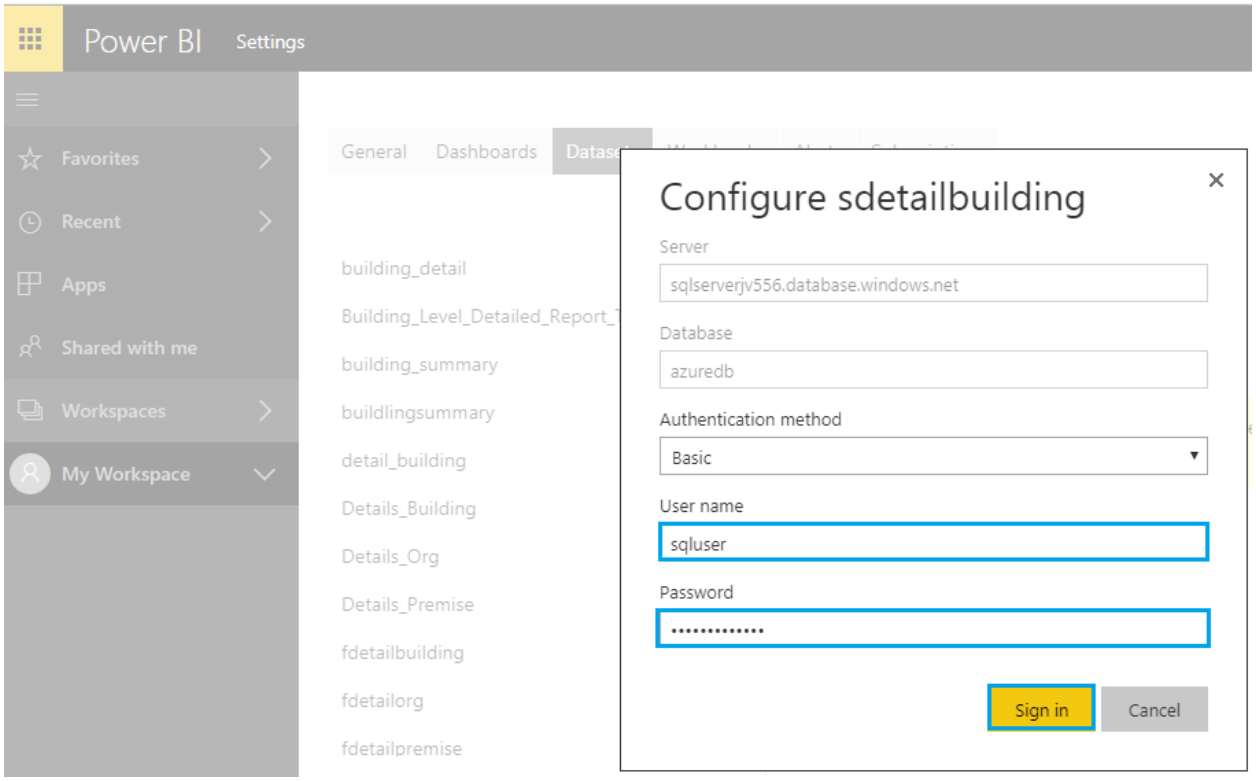
33. Click on **Publish** when you view the graph.



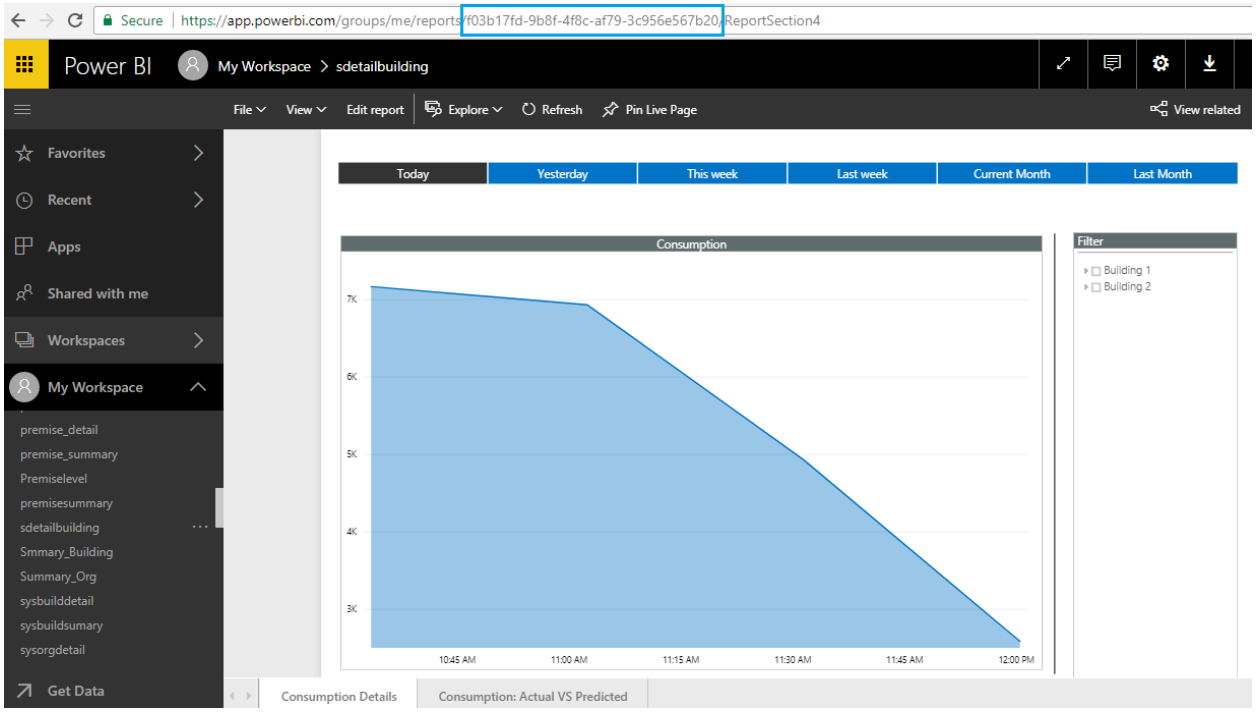
34. Click on **Enter credentials.**



35. Enter the Azure SQL Server **User name** and **Password.**



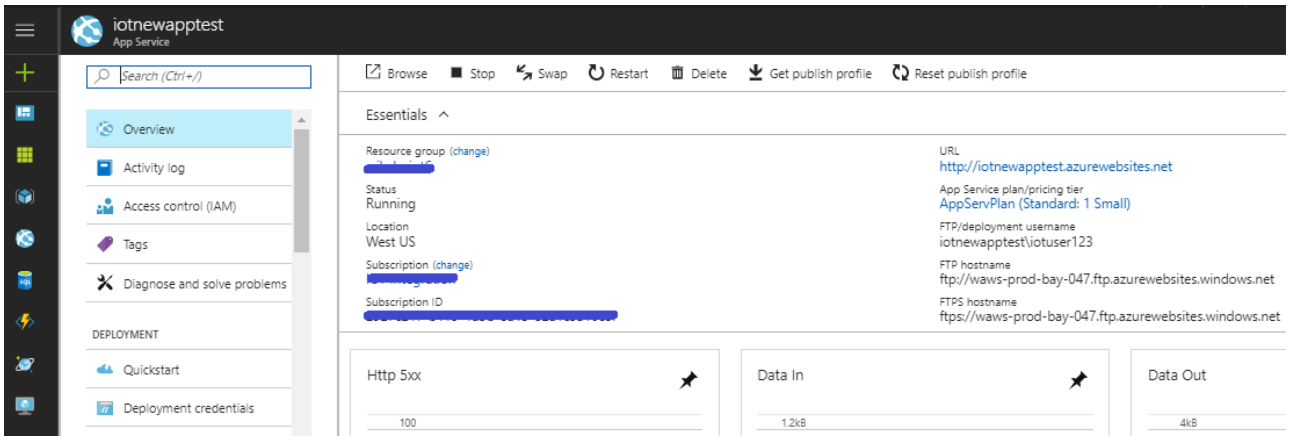
36. Copy the token from the URL after publishing each template and save it for further configuration in the web app.



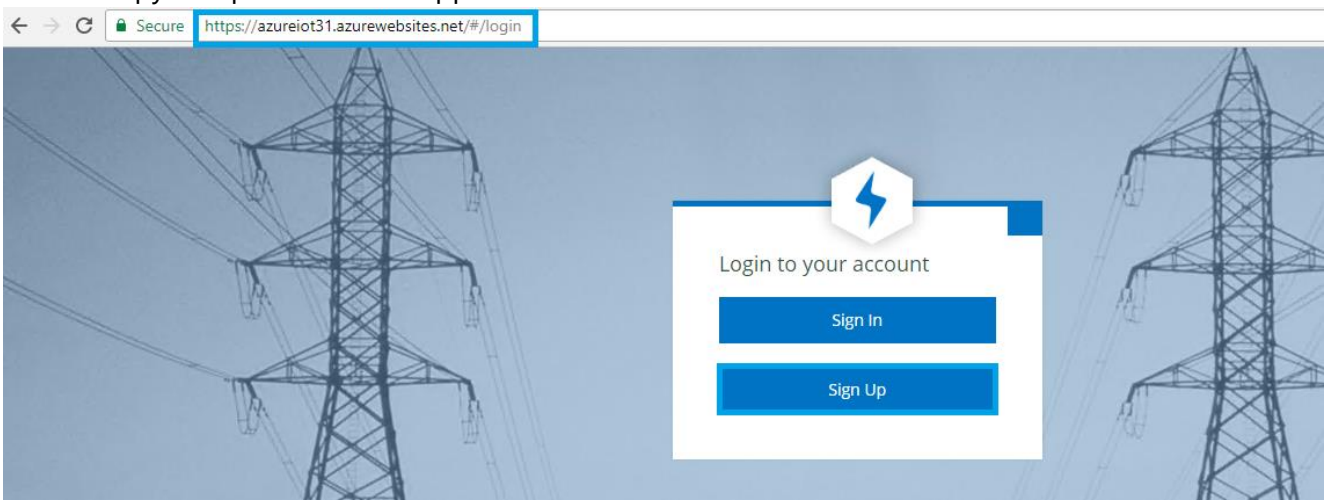
37. Repeat the same steps for organization and feedback detailed reports.

11. Configuring and Accessing the Webapp

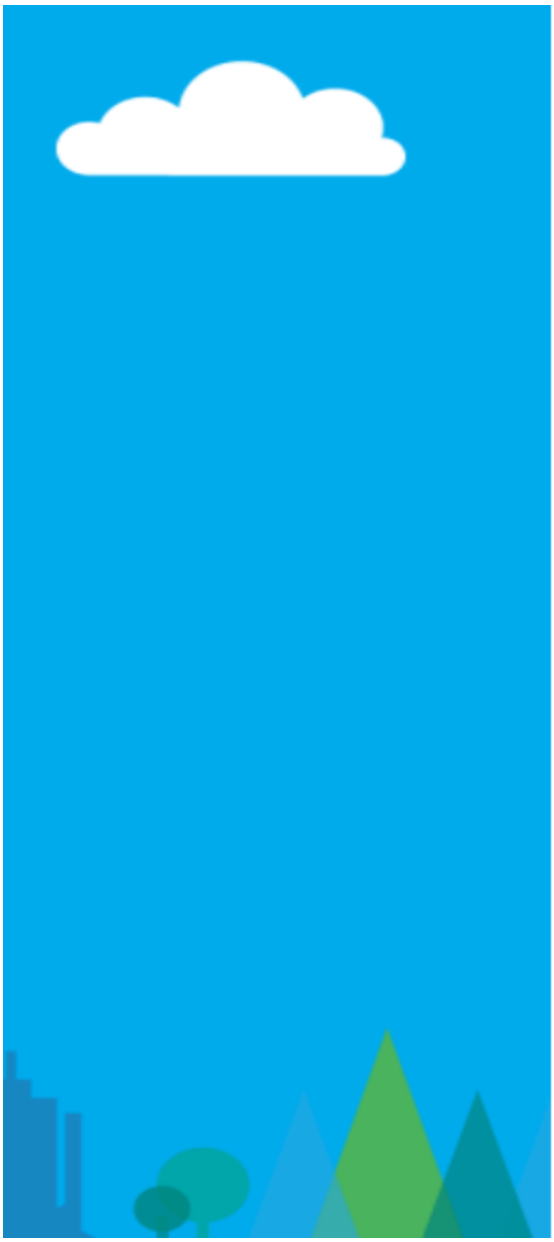
1. Go to the Web Application in the Resource Group and copy the addess listed under "**URL**".



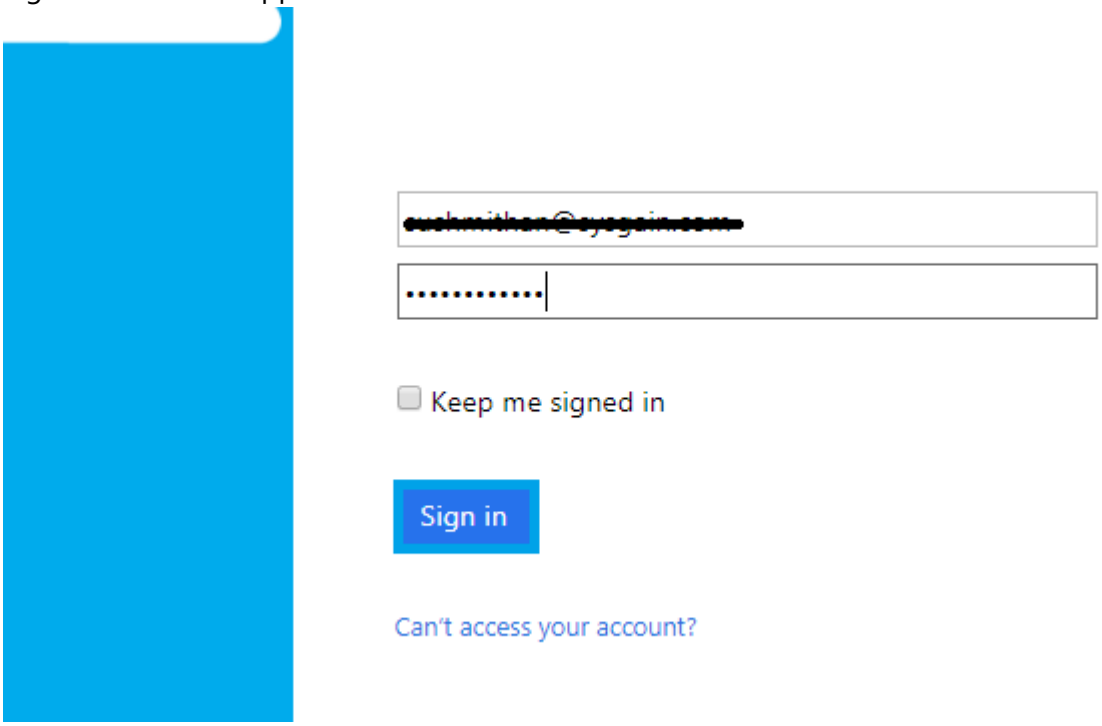
2. Copy and paste the web app url in a new browser.



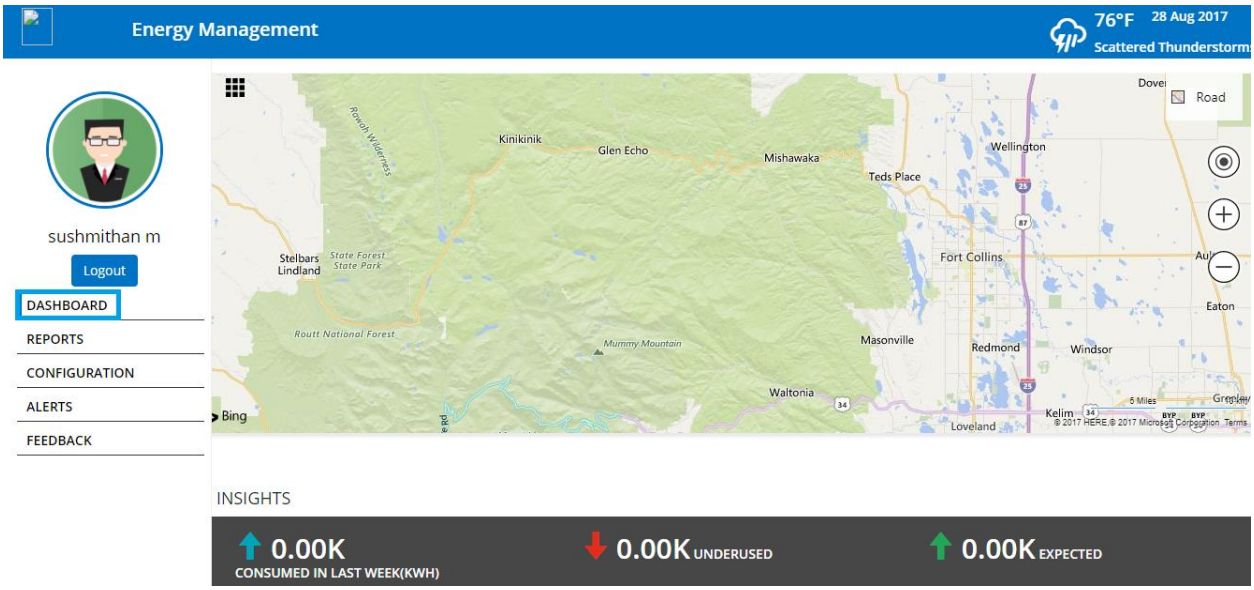
3. Login using the web application credentials if you already have an account. If you don't, click on Account Sign Up.
4. Click on **Sign Up** to access the Web app. You will receive a verification code in your email. Enter it, then click on **Verify Code**. Enter the other details and click on **Create**.


Email Address
Verification code
519025
Verify code
Send new code
New Password
Confirm New Password
Surname
Street Address
8638 154th Ave NE
State/Province
Washington
Postal Code
98052
Job Title
DevopsEngineer
Given Name
Display Name
Country/Region
United States
City
Redmond
Create
Cancel
Activate Windows
Go to Settings to activate Windows.

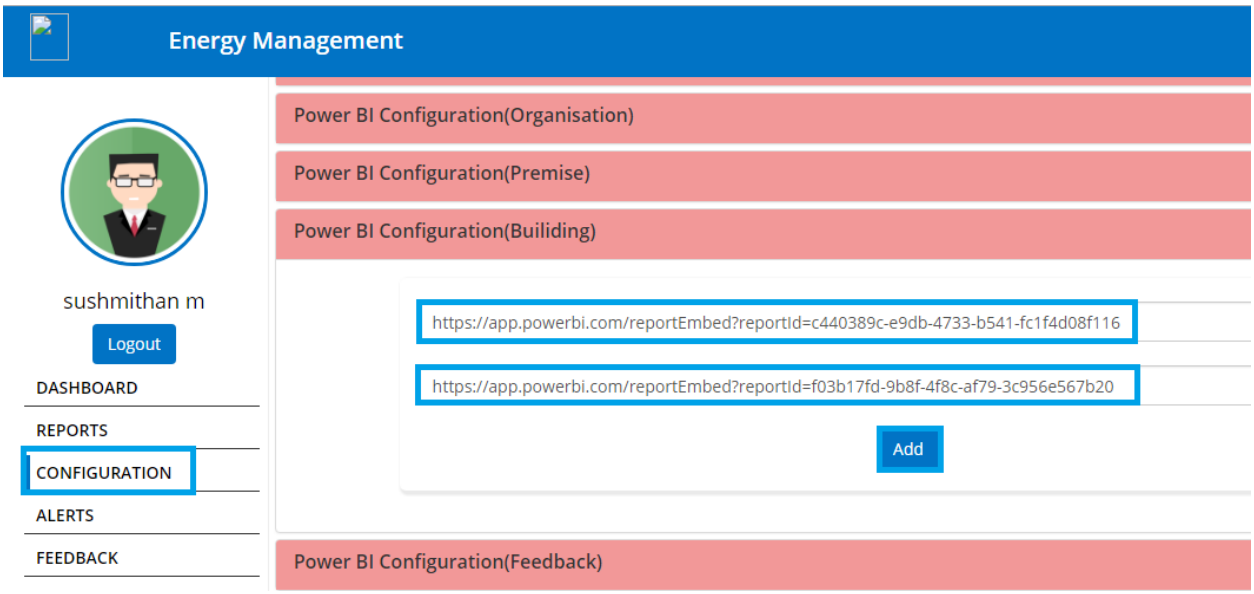
4. Sign in to the web app with the credentials created.



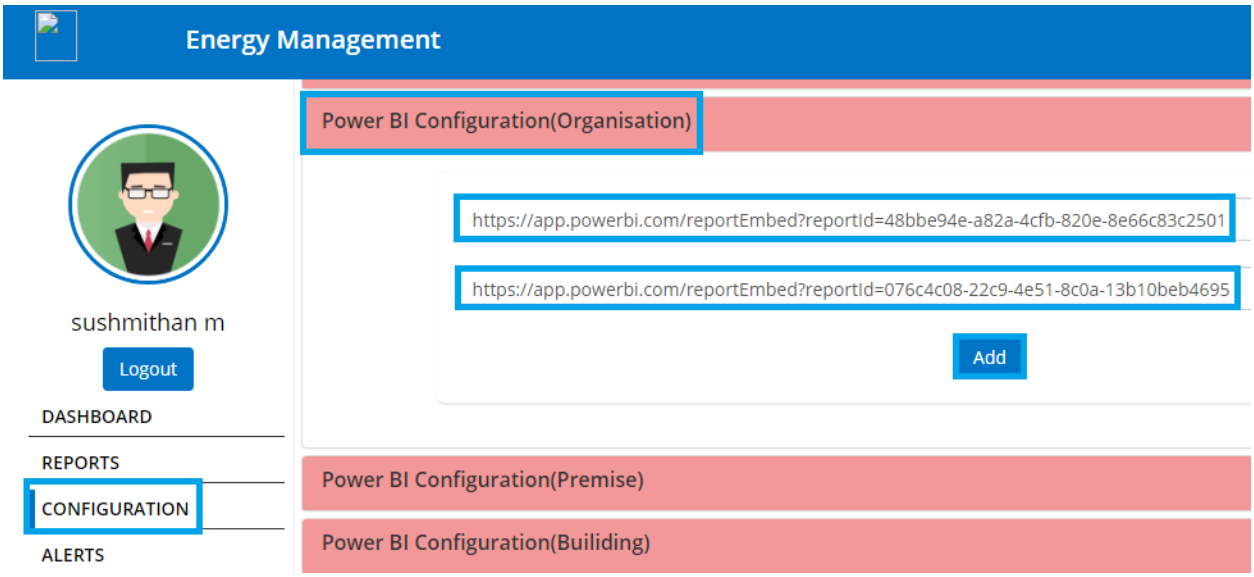
5. Once in the web app, you can view the **Dashboard** as shown below.



6. To configure the Power BI (**Building**), make the URL by using the Power BI tokens in the below format:
   https://app.powerbi.com/reportEmbed?reportId=<token>
   Enter them in the respective tabs (summary reports in the first column, detailed report in the second column), then click on **Add.**

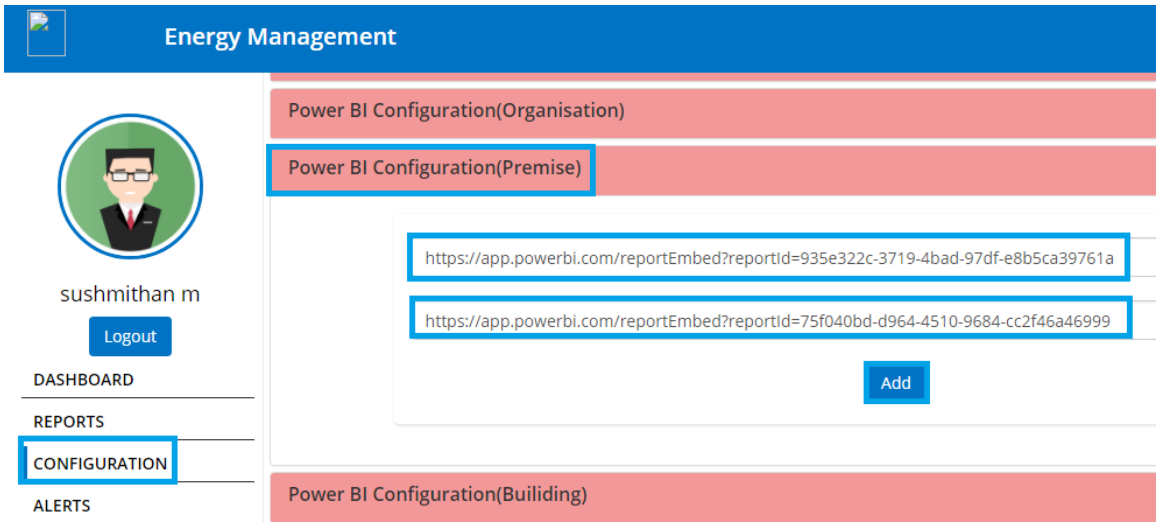


7. To configure the Power BI (**Organization**), make the URL by using the Power BI tokens in the below format:
   https://app.powerbi.com/reportEmbed?reportId=<token>
   Enter them in the respective tabs (summary reports in the first column, detailed report in the second column), then click on **Add.**

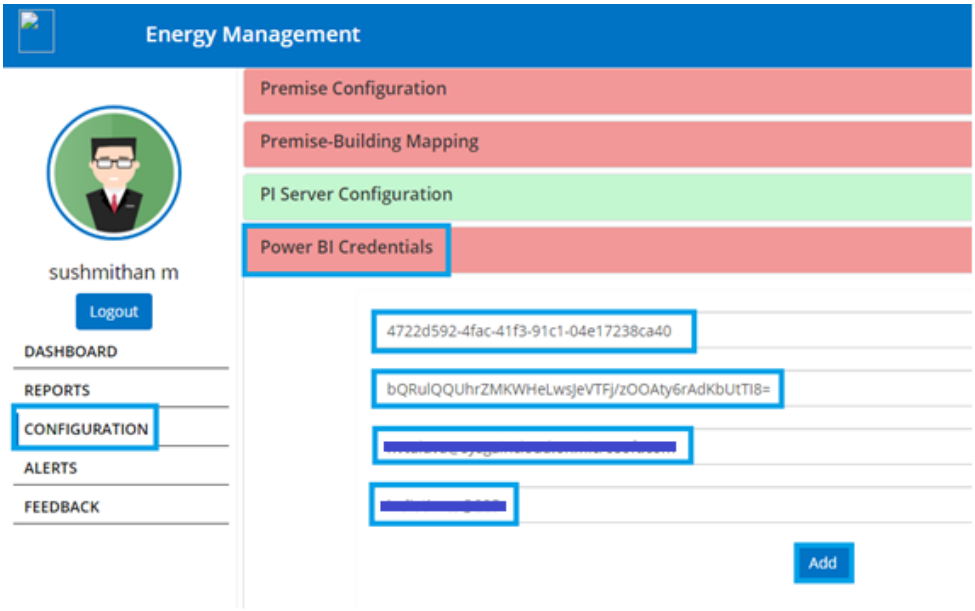


8. To configure the Power Bi (**Premise**), make the URL by using the Power BI tokens in the below format:

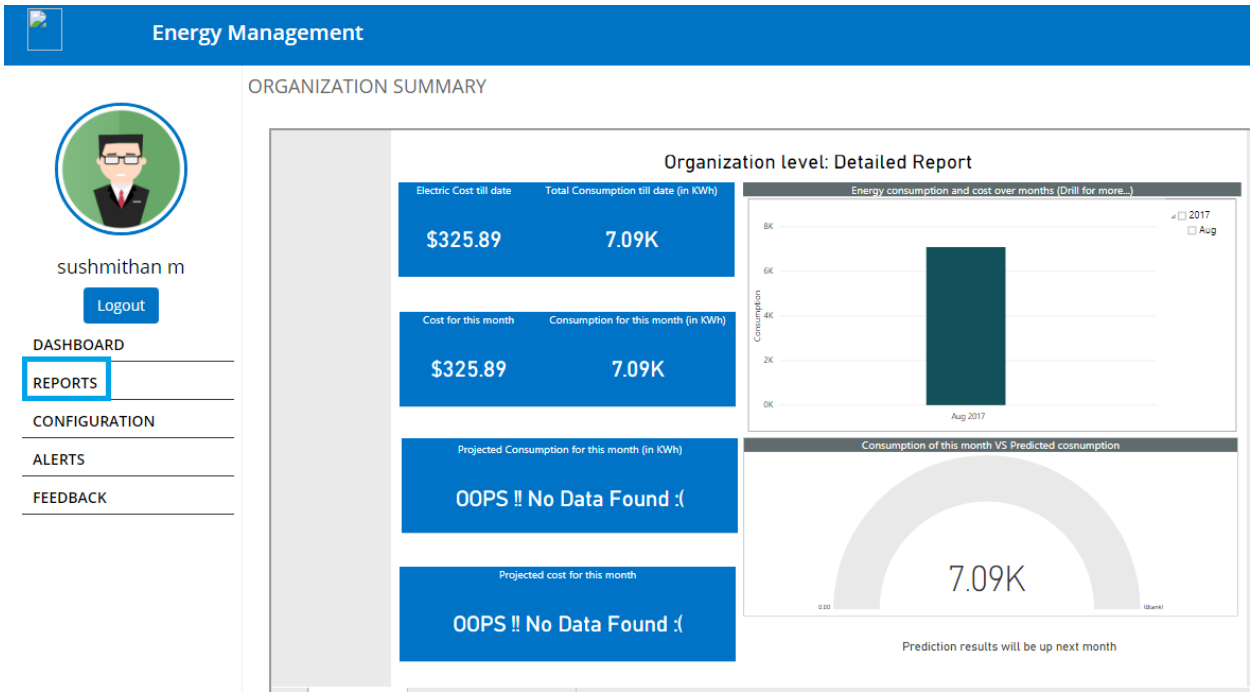
https://app.powerbi.com/reportEmbed?reportId=<token>
Enter them in the respective tabs (summary reports in the first column, detailed report in the second column), then click on **Add.**

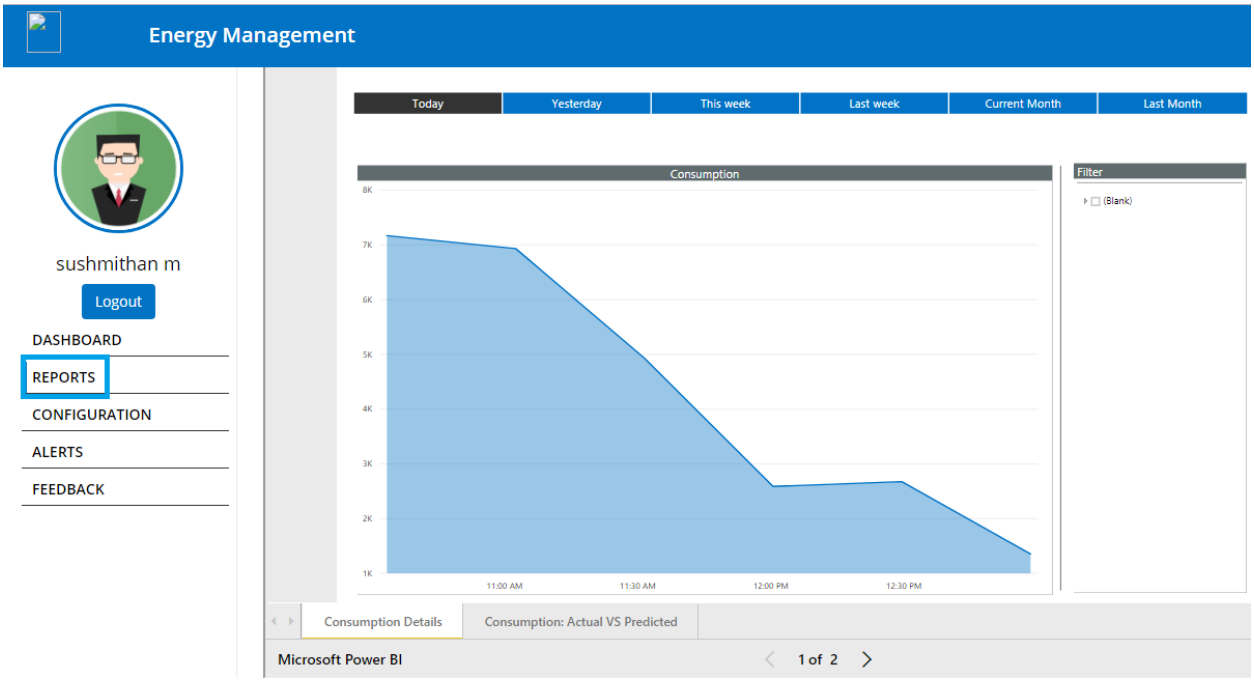


9. Enter the details of the Power BI which were used to register the **Power BI** with the web app and the **client id** and **client secret** which we got after resetting the app. Click on **Add.**



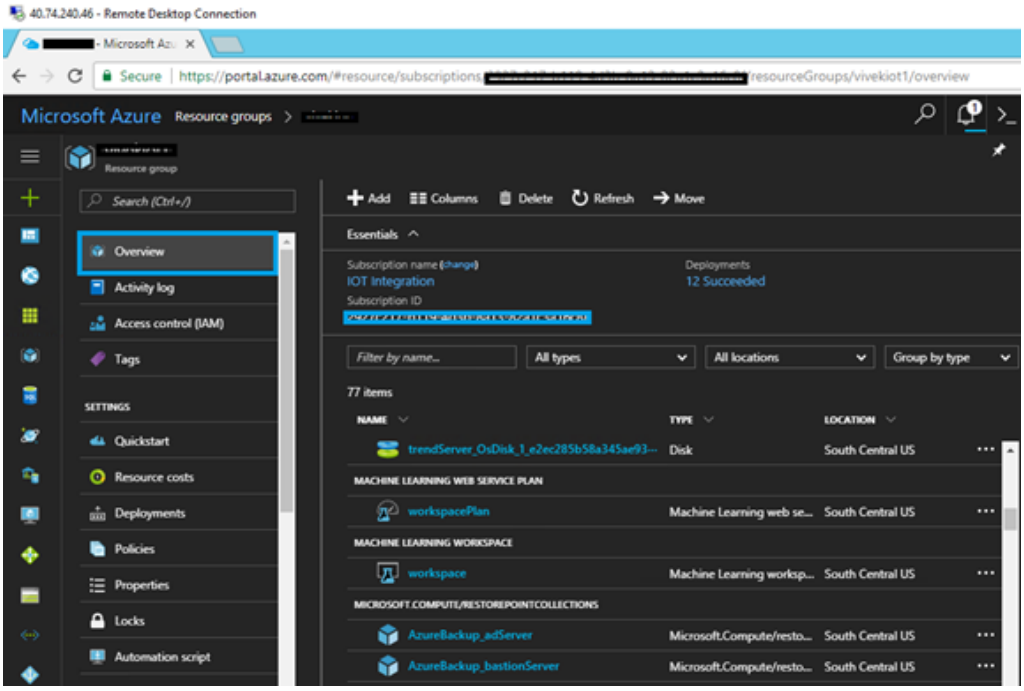
10. Click on **Reports** to view the graph of the data.



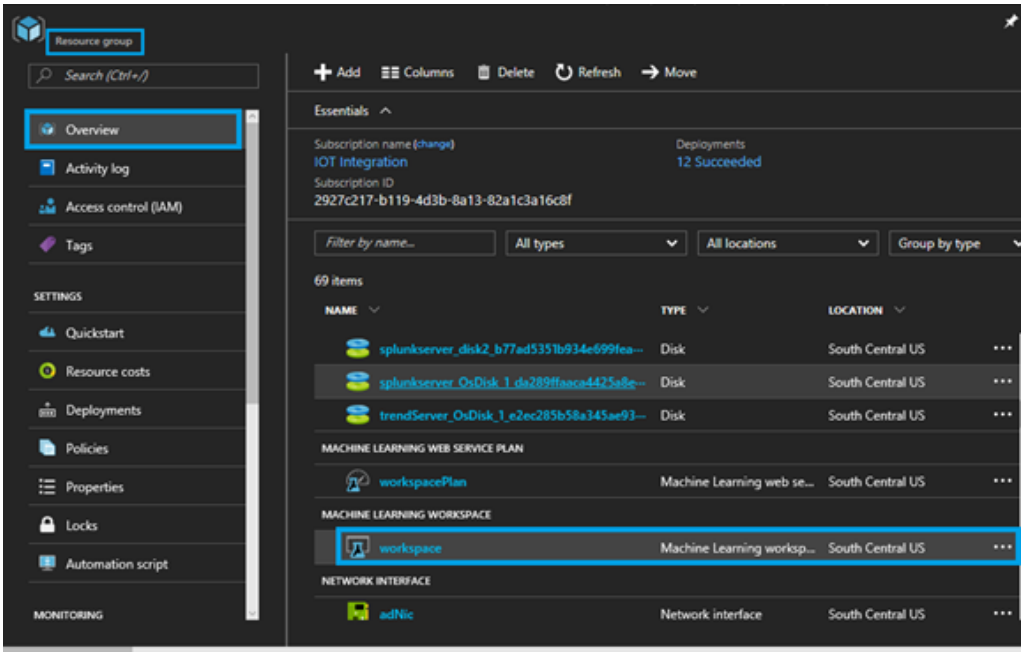


12. Machine Learning Experiment

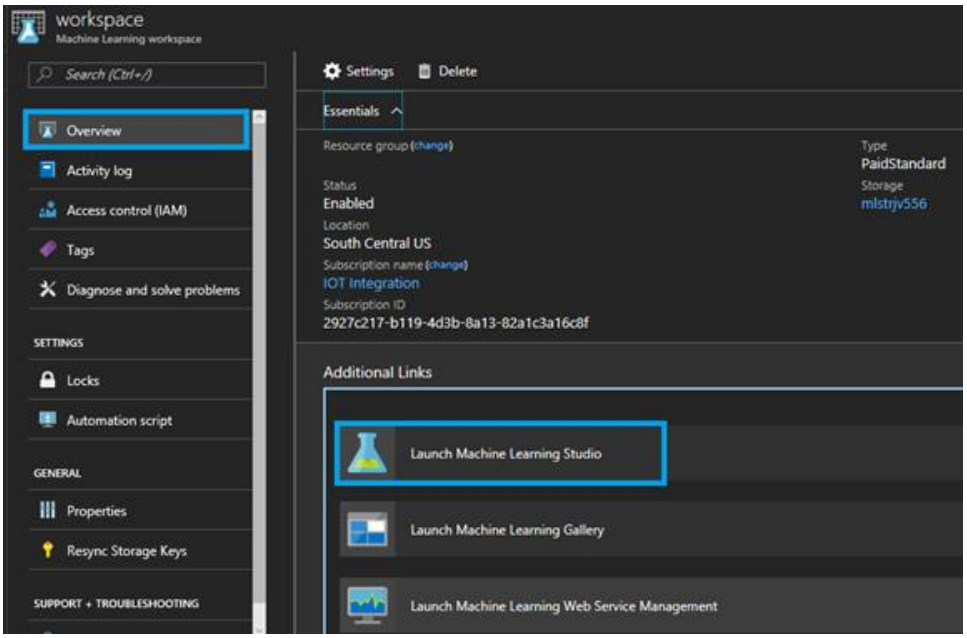
1. Log in to the Bastion host and open the Azure Portal. Navigate to the Resource Group.



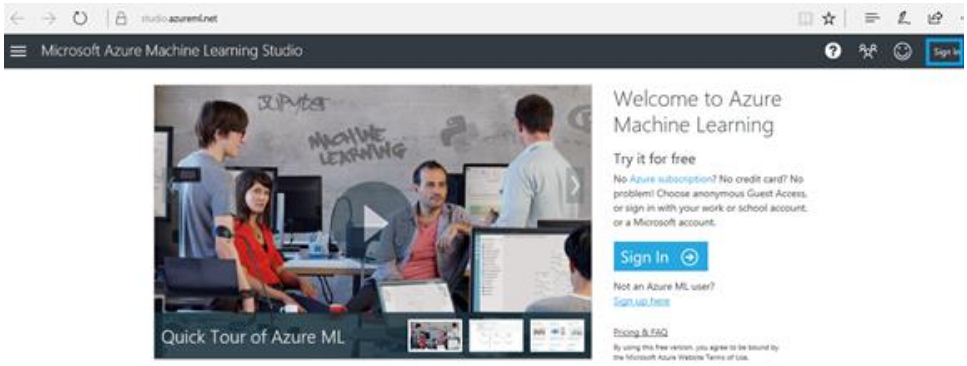
2. Click on the **workspace**.



3. Click on **Launch Machine Learning Studio**.

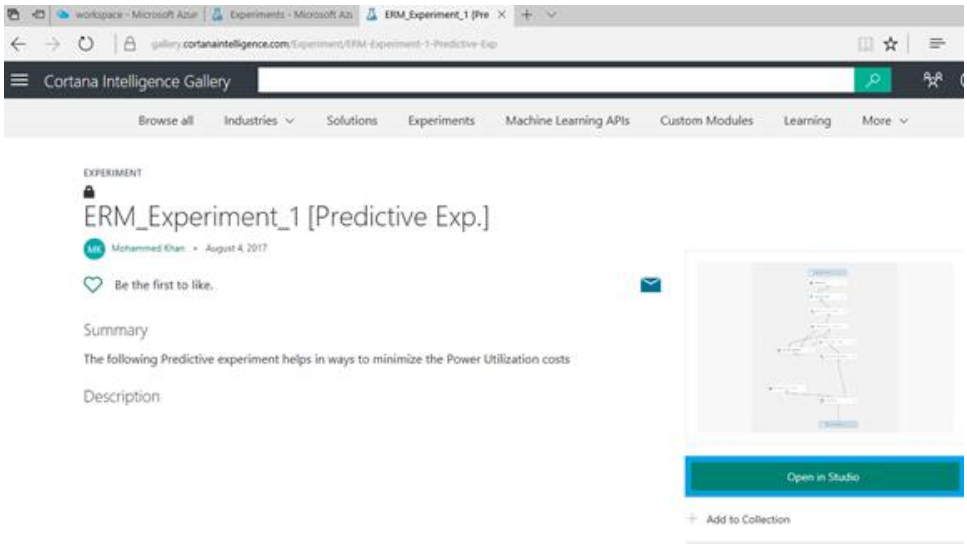


4. Sign in to the **Microsoft Azure Machine Learning Studio**.

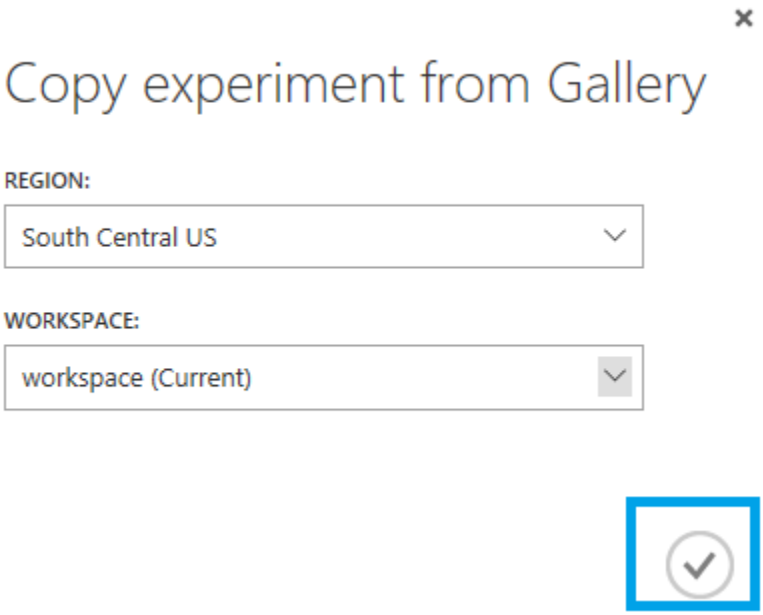


5. Open the below URL in a new browser and click on **Open in Studio**. This will launch the Experiment to the **workspace**.

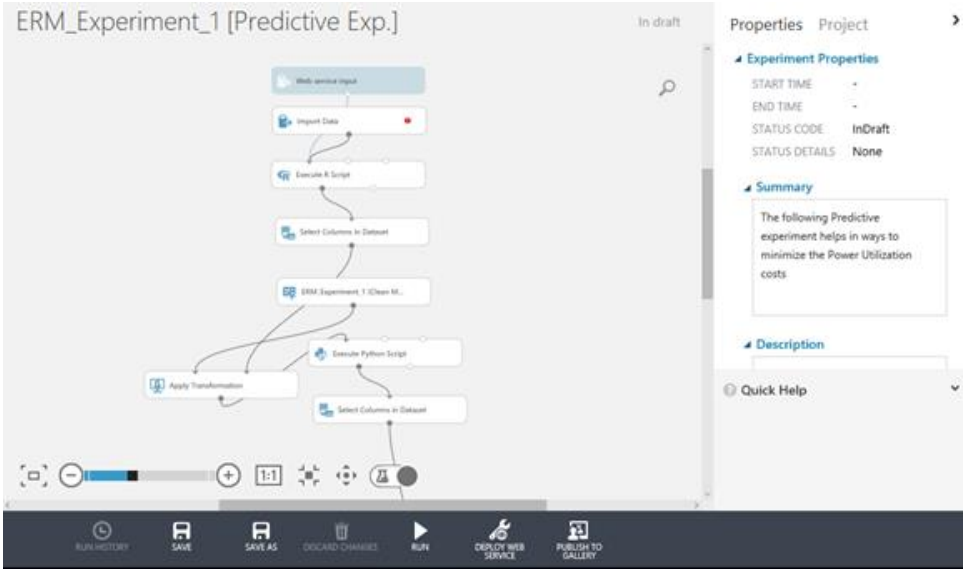
Path : https://gallery.cortanaintelligence.com/Experiment/ERM-Experiment-1-Predictive-Exp



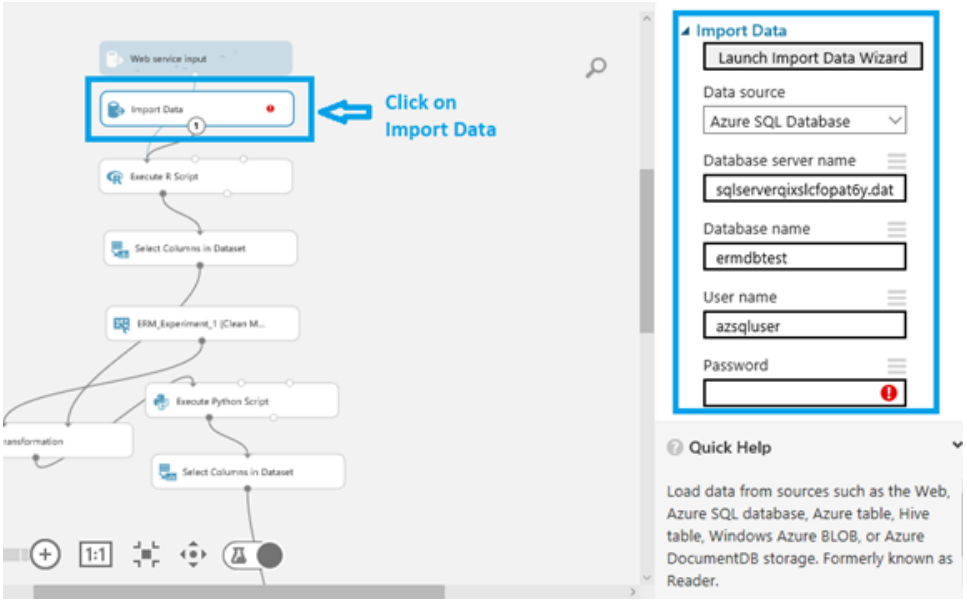
6. The below screen will appear in the new tab, click on the **check mark**.



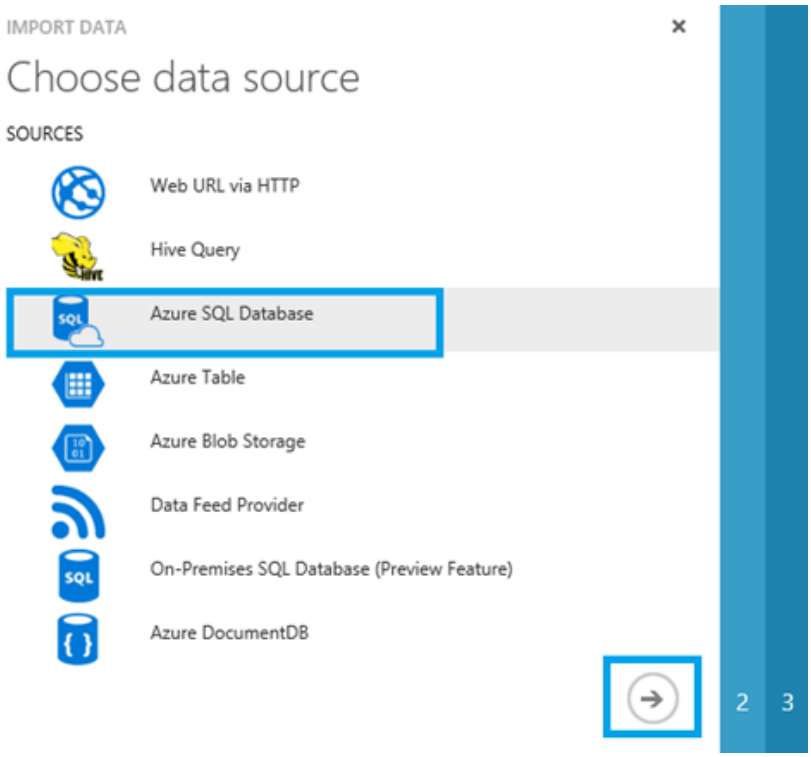
7. The experiment will be downloaded to the workspace.



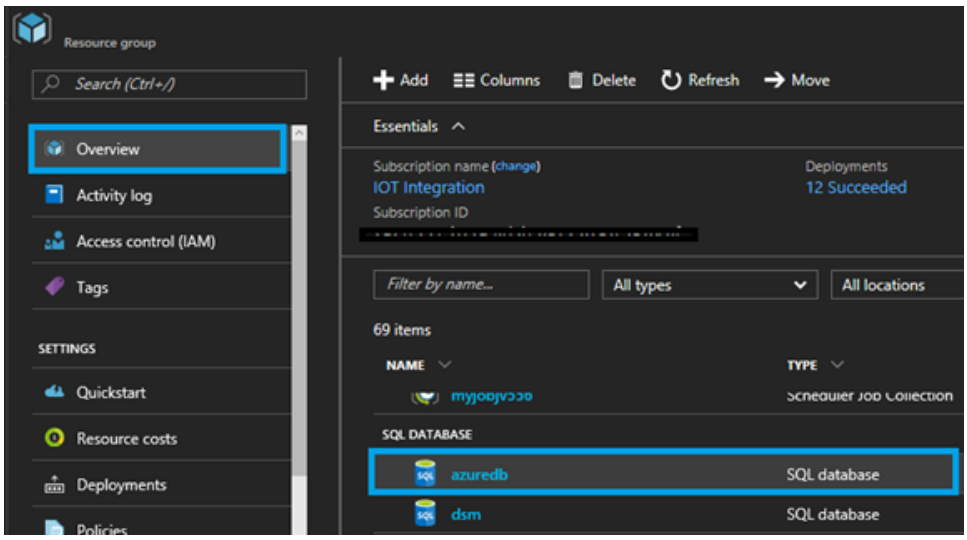
8. Once the experiment is pulled into the workspace, click on **Import Data**. Then click on **Launch Import Data Wizard** from right side menu.



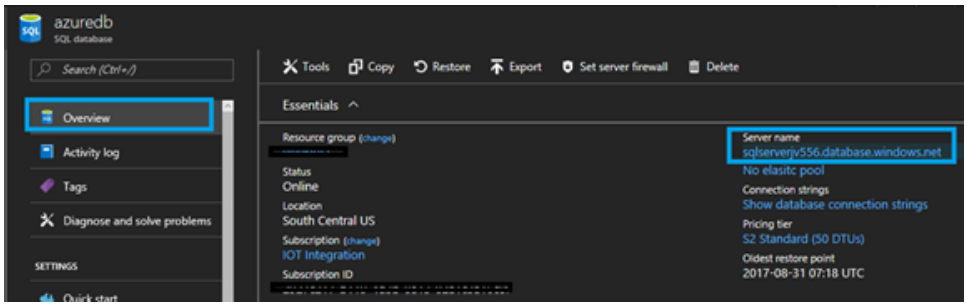
9. Select **Azure SQL Database** and click on Next icon **"->".**



10. Click on **azuredb** under **SQL DATABASE**.



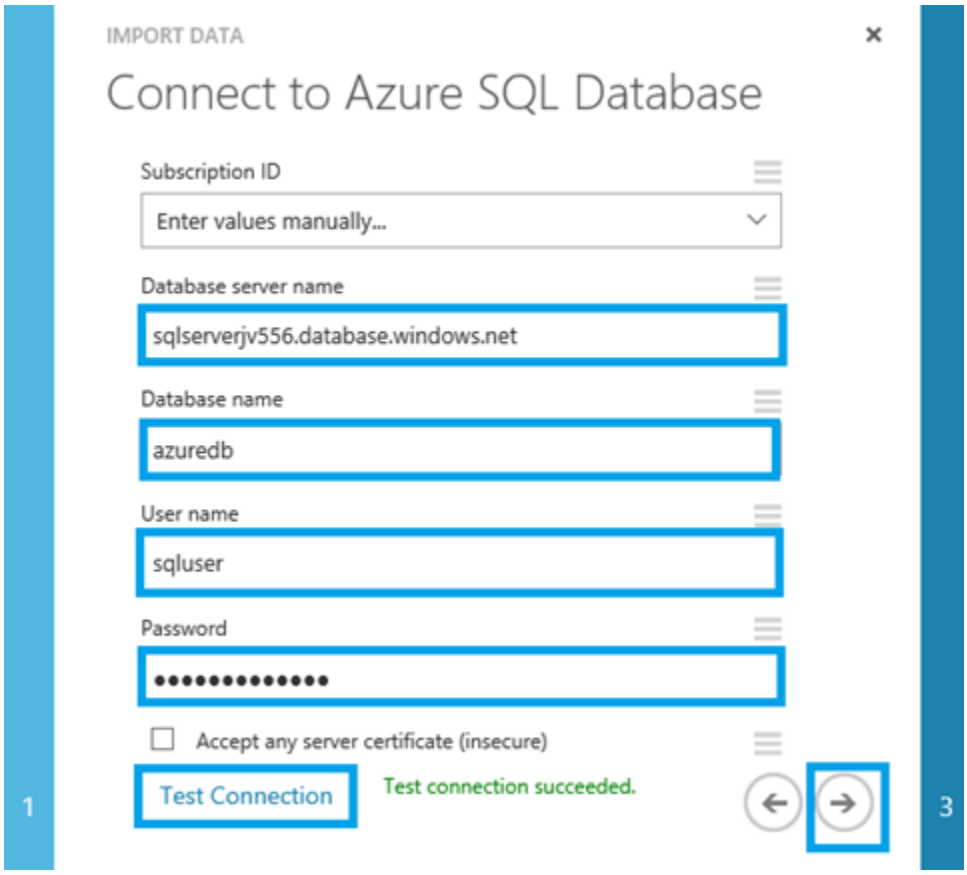
11. Open the Database **Server name**.



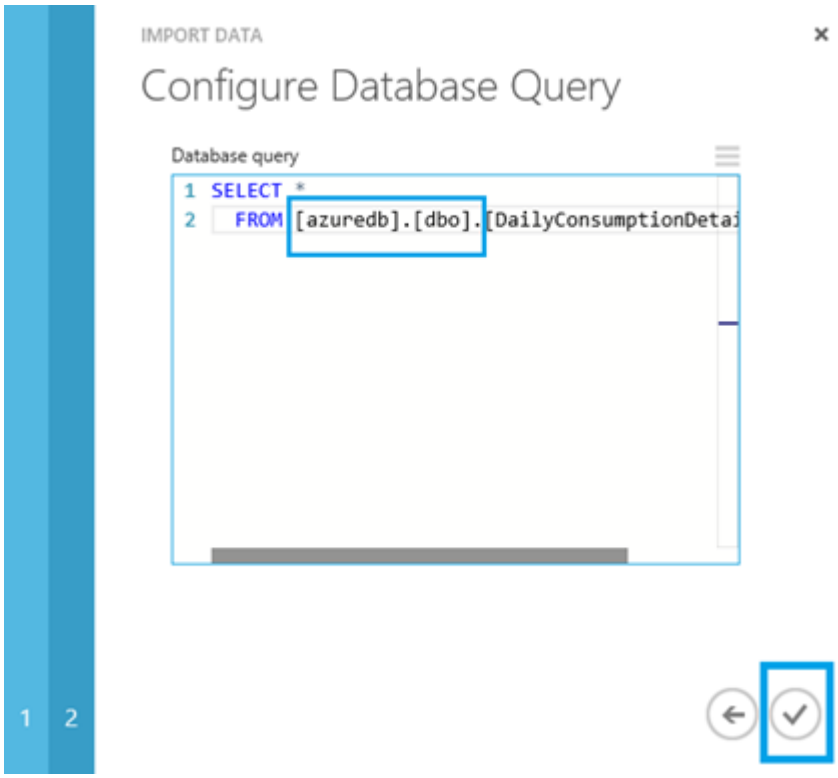
12. In the below screen, paste the **Database server name**.

Enter the **Database name**, **User name,** and **Password,** then click on **Test Connection**.

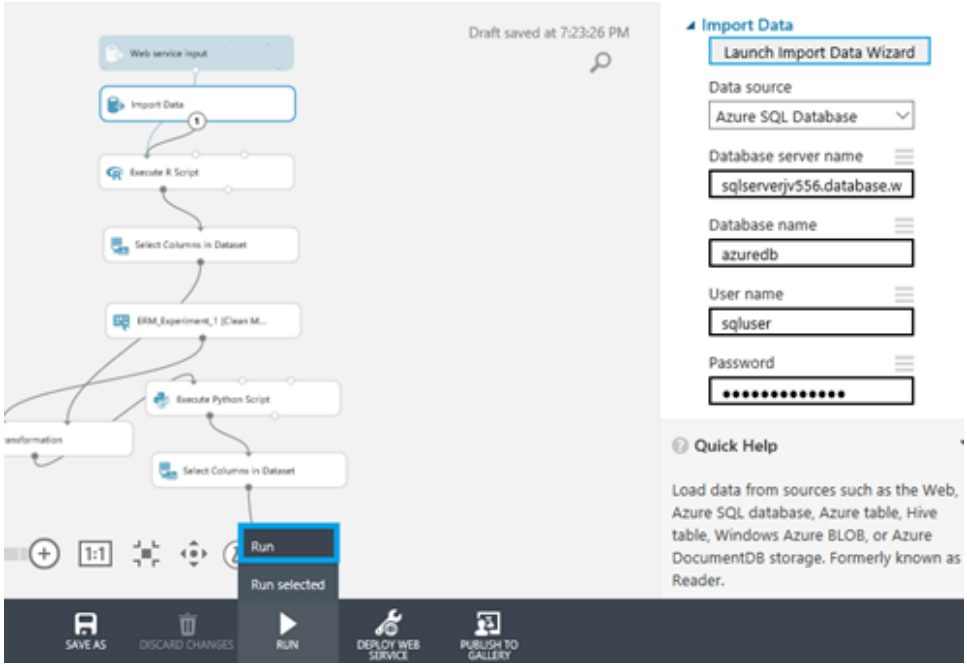
After the test connection succeeds, click on Next icon.



13. Replace the Database name with **azuredb** and click on the **check mark.**

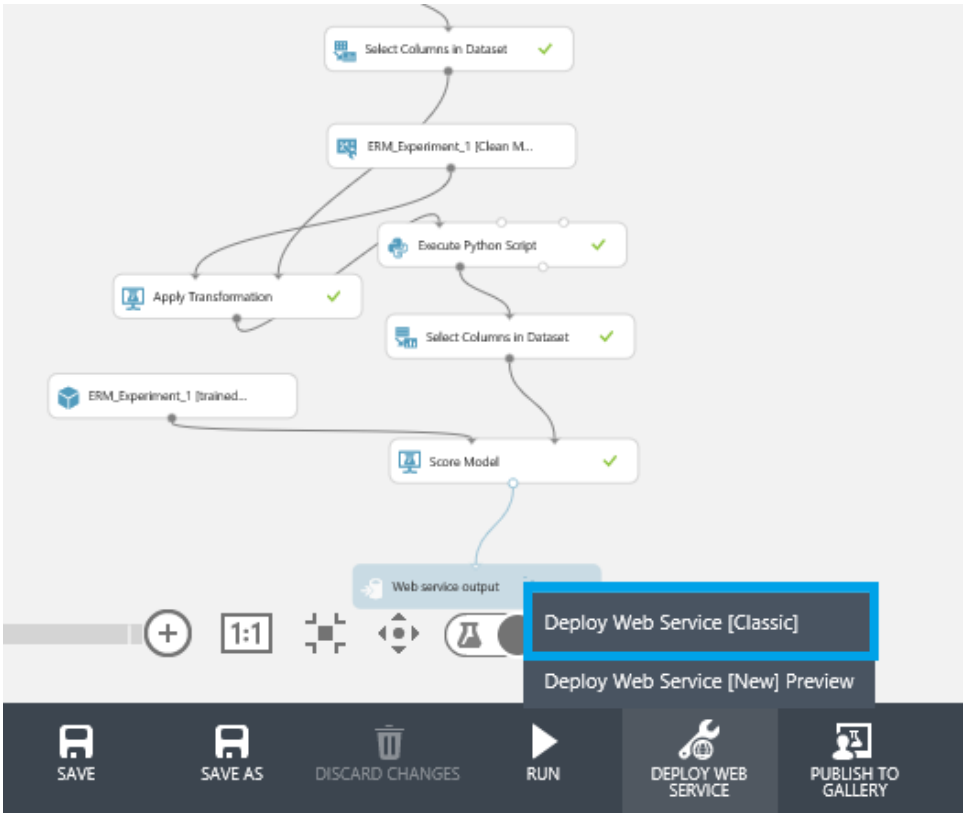


14. Once done, run the experiment by right clicking on **Run** from bottom of the below screen, and select **Run** from the dropdown menu.

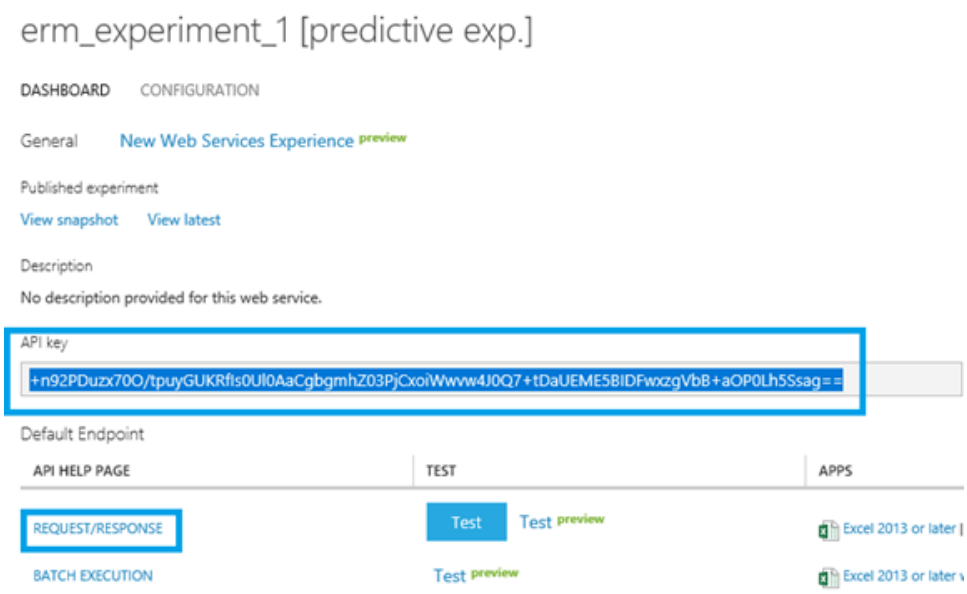


15. After running the experiment successfully, we will get **finished running** on right side of the screen.

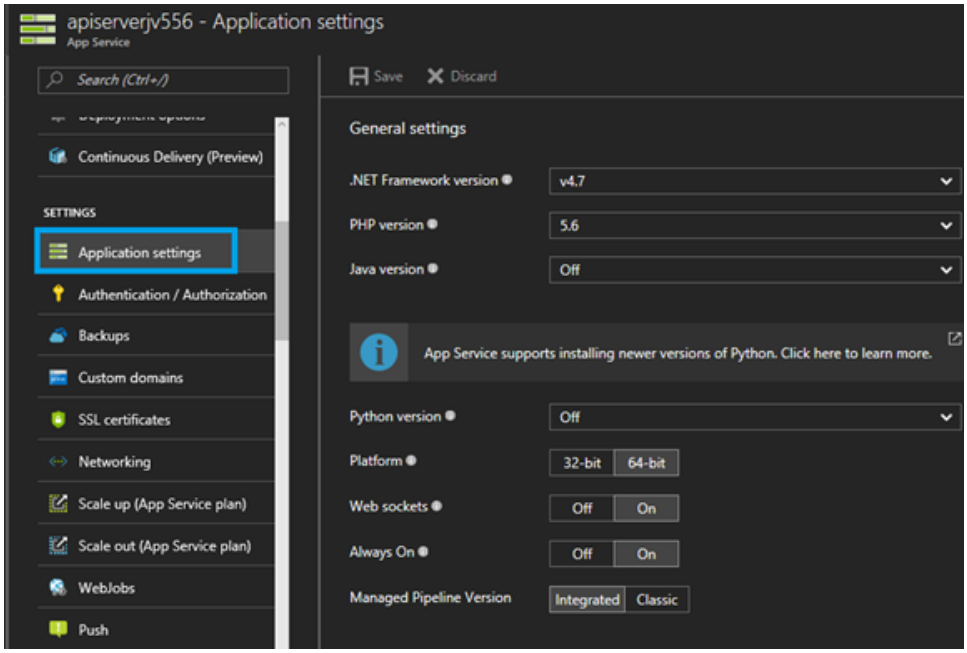
16. Right click on **Deploy Web Service** button from the bottom of the screen and click on **Deploy Web Service [Classic]** to publish the experiment as a web service in classic mode.



17. Once the experiment is deployed, the below screen will appear. Copy the **API Key** and save it for later use.
18. Click on **Request/Response** under **API HELP PAGE** to get the **POST URL**.



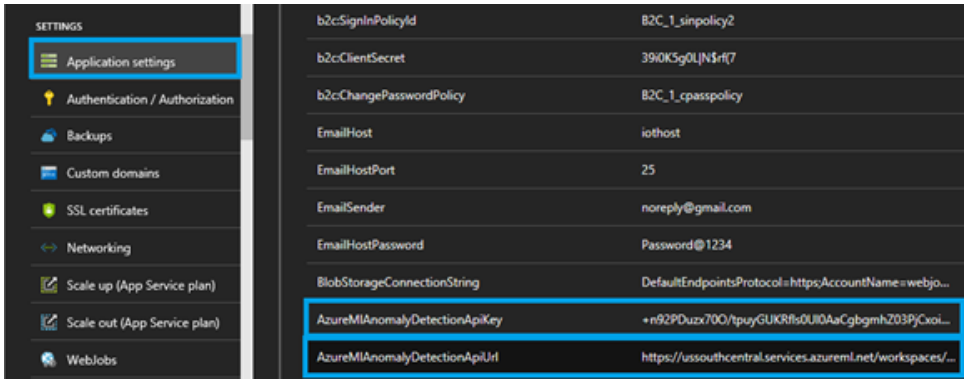
19. Copy the POST URL and save it for later use.
20. Navigate to **Application settings** of **apiserver** webapp and scroll down to **App Settings**.



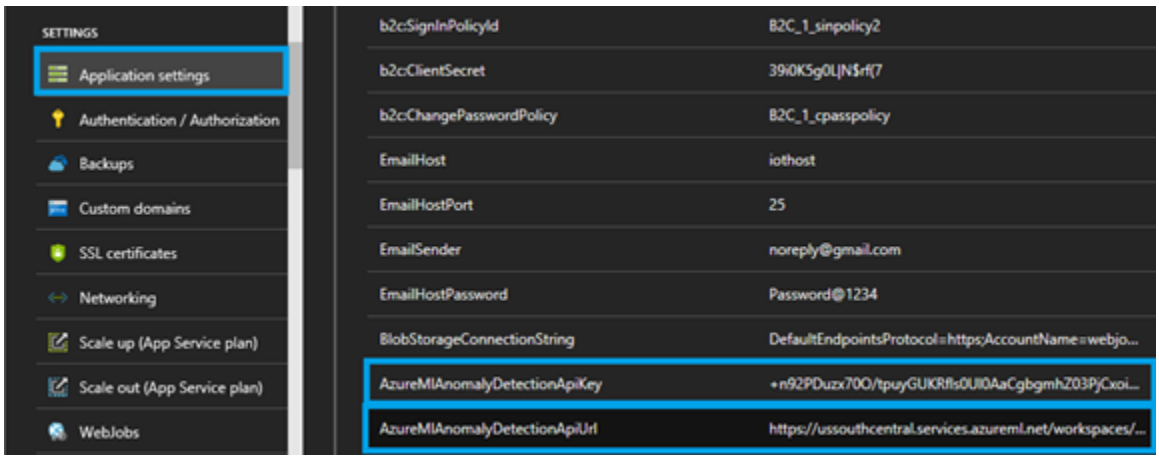
21. Add

    AzureMlAnomalyDetectionApiKey with apikey value from **step 17**.

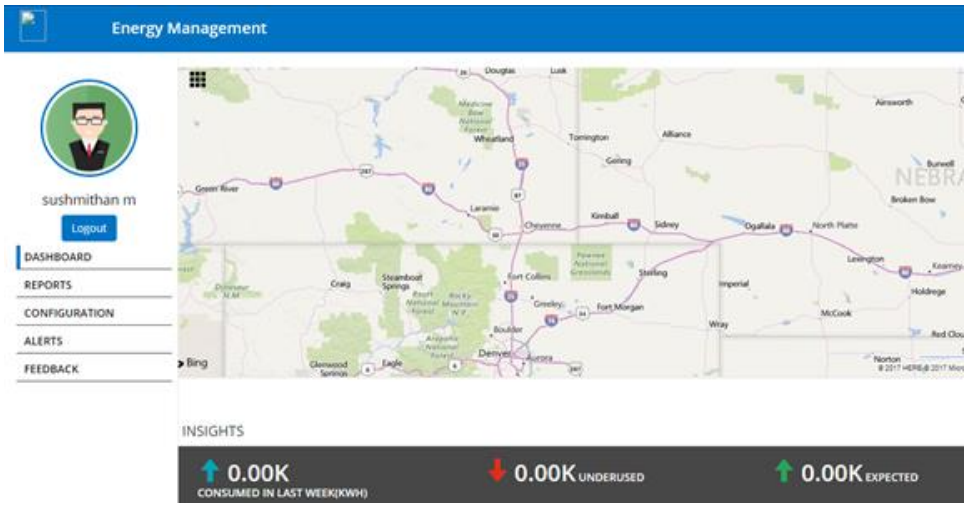
AzureMlAnomalyDetectionApiUrl with Post URL from **step 18**.



22. Restart the **apiserver**.

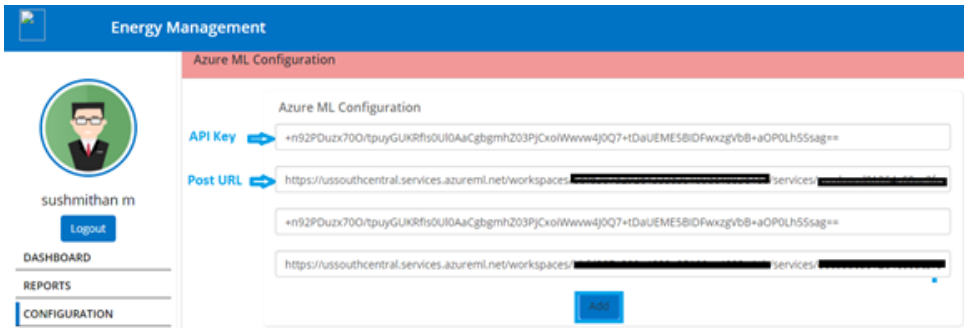


23. Login to the web application.

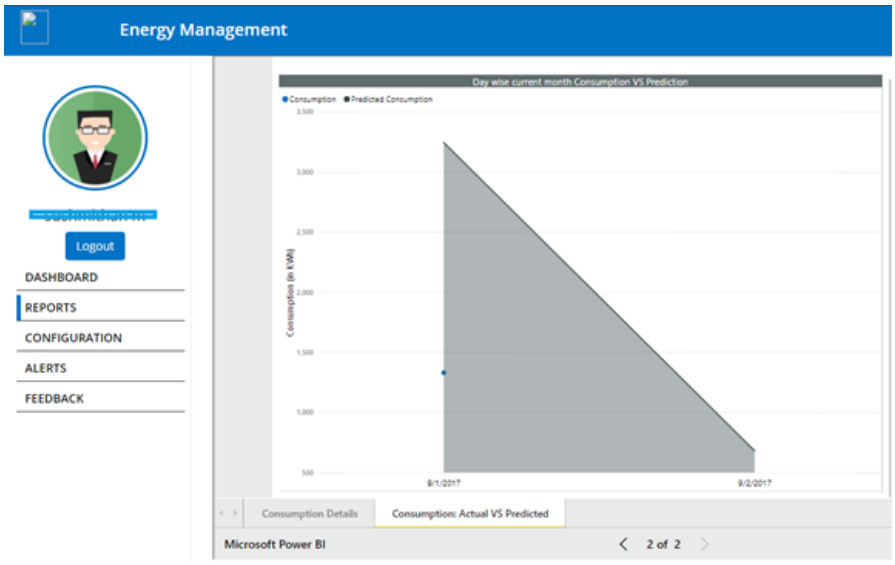


24. Navigate to **Azure ML Configuration** and add the **API Key** and **POST URL**.

Click on **Add**.

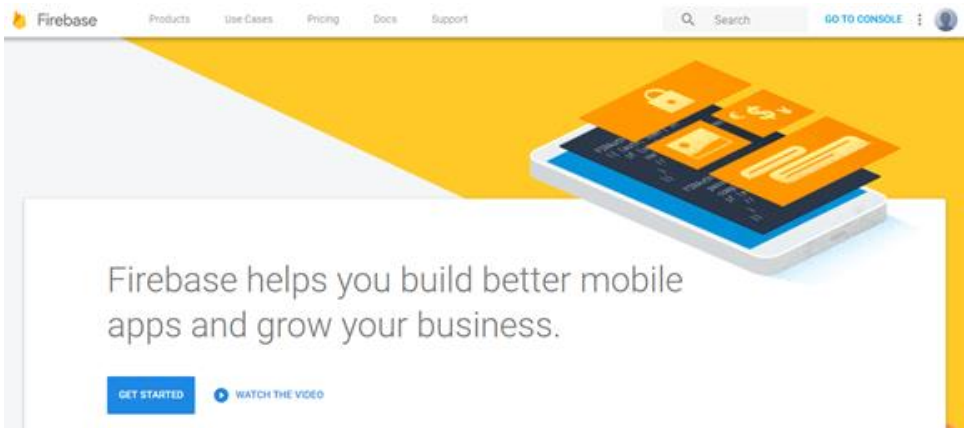


25. Click on **REPORTS** and click on **Consumption: Actual VS Predicted** of the bottom of the screen to view the Actual Vs Predicted graph.

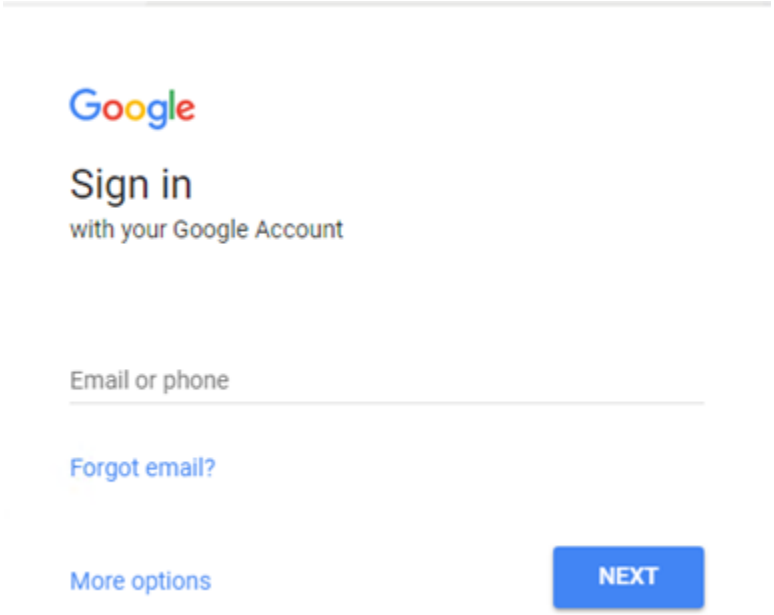


13. Firebase Configuration

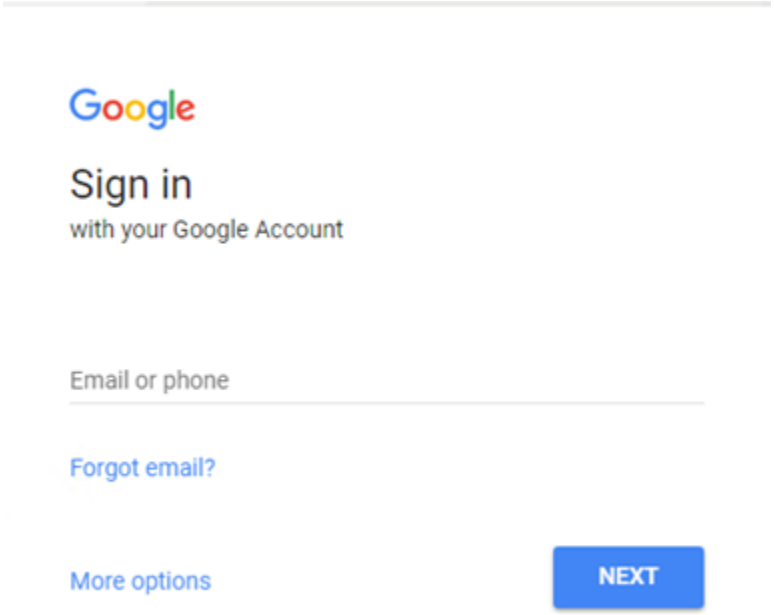
1. Go to the https://firebase.google.com URL and click on **GO TO CONSOLE**.



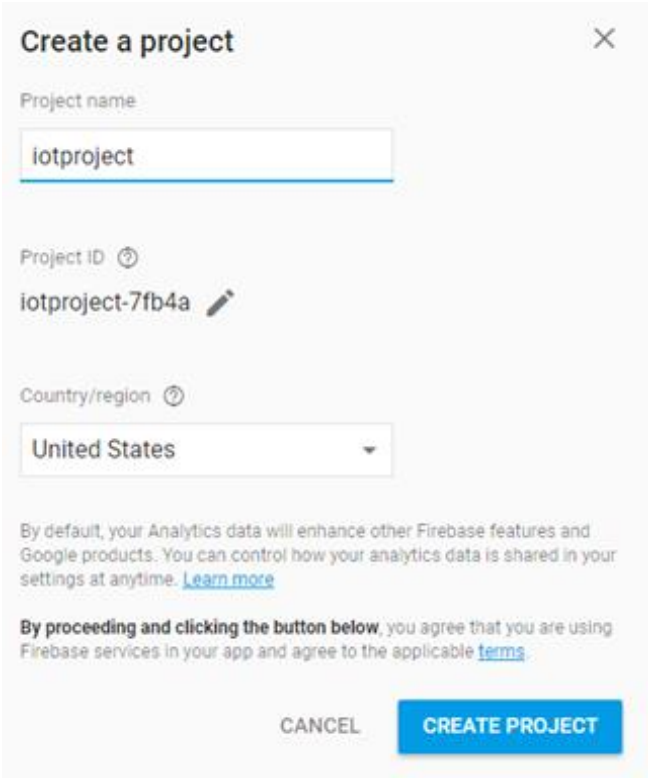
2. Sign in with your Gmail credentials.



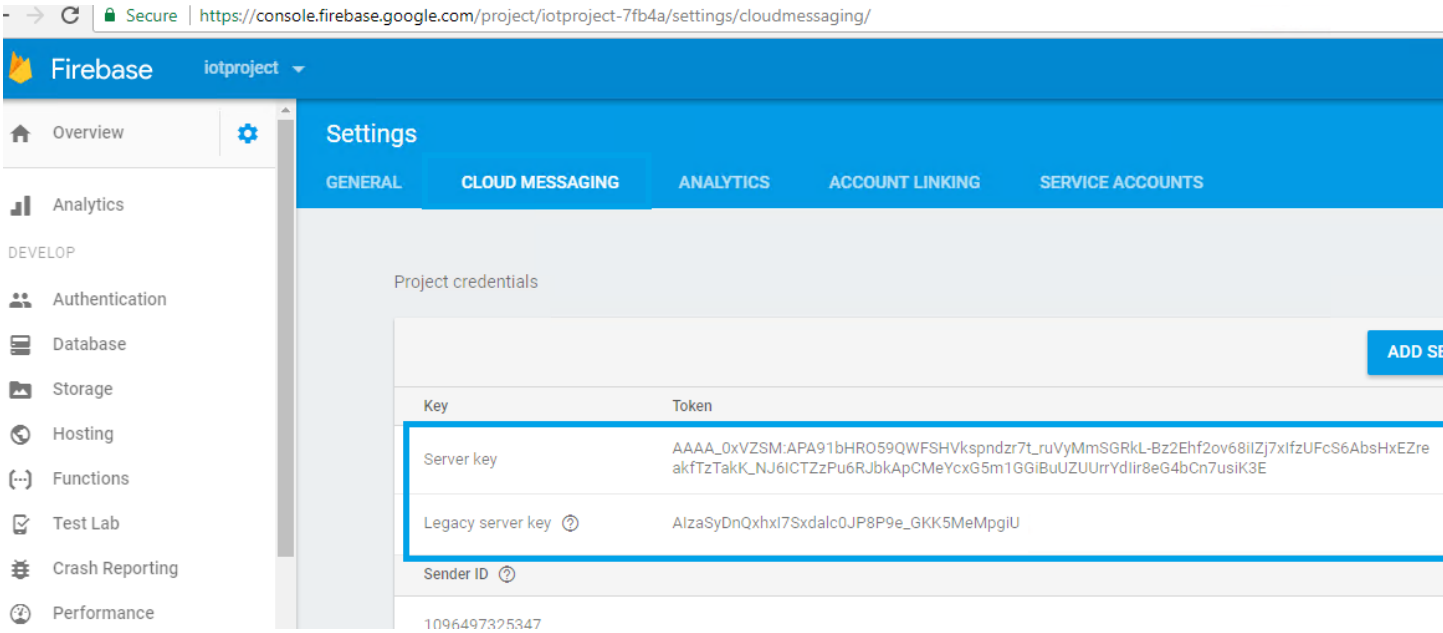
3. Click on **Add Project**.



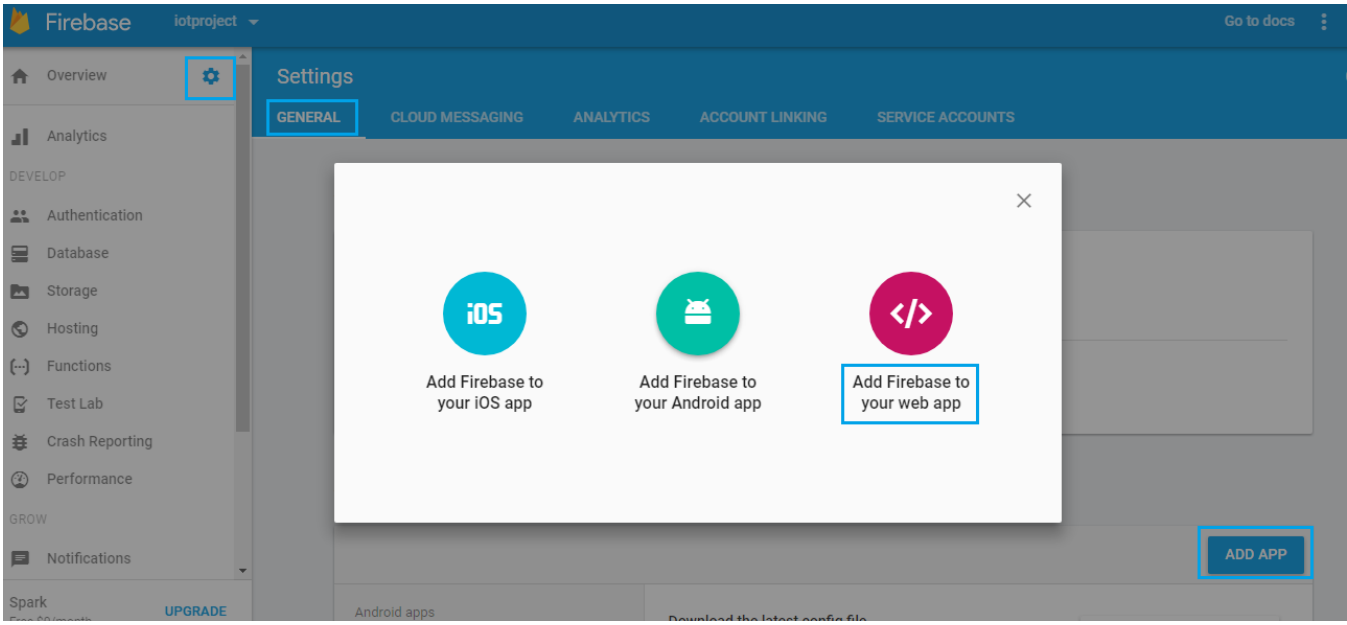
4. Give a **Project name** and click on **CREATE PROJECT.**



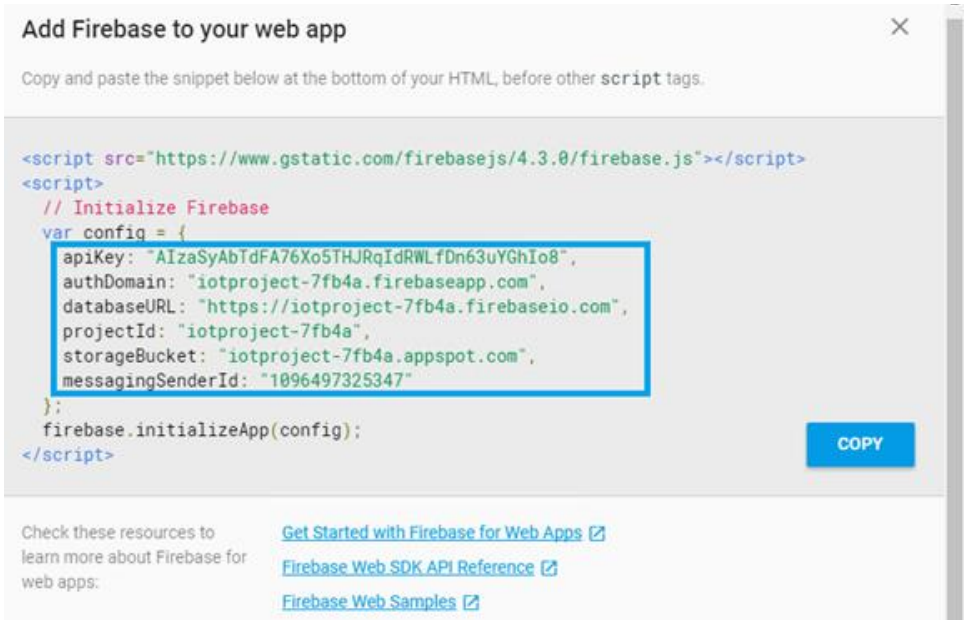
5. Navigate to **Settings** > **Project settings** > click on **CLOUD MESSAGIN.**
6. Save the **Server key** and **Legacy Server Key.**



7. To Register Firebase with a WEB APP, navigate to **settings** > **GENERAL** > click on **Add Firebase to your Web App** by click on Add App.



8. A pop up window appears. Copy and save the code snippet below and enter the credentials in the Web App.




```
<script src="https://www.gstatic.com/firebasejs/4.3.0/firebase.js"></script>
<script>
 // Initialize Firebase
 var config = {
   apiKey: "AIzaSyAbTdFA76Xo5THJRqIdRWLfDn63uYGhIo8",
   authDomain: "iotproject-7fb4a.firebaseapp.com",
   databaseURL: "https://iotproject-7fb4a.firebaseio.com",
   projectId: "iotproject-7fb4a",
   storageBucket: "iotproject-7fb4a.appspot.com",
   messagingSenderId: "1096497325347"
 };
 firebase.initializeApp(config);
</script>
```

9. Open postman

- Change the Params to **POST** and paste the below URL

  https://fcm.googleapis.com/fcm/send

- Click on Body and enter the following:

  {

  "data":{

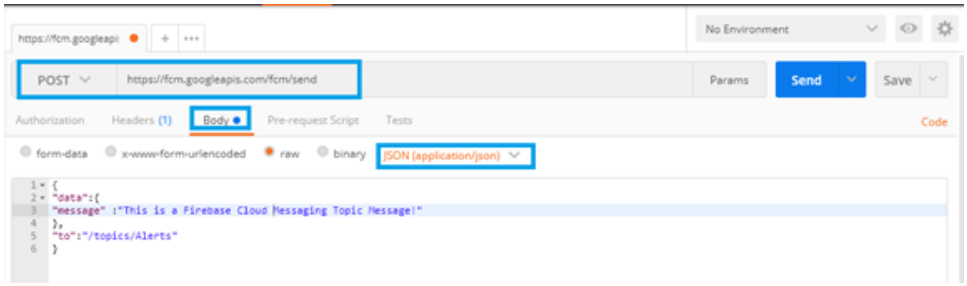
  "message" :"This is a Firebase Cloud Messaging Topic Message!"

  },

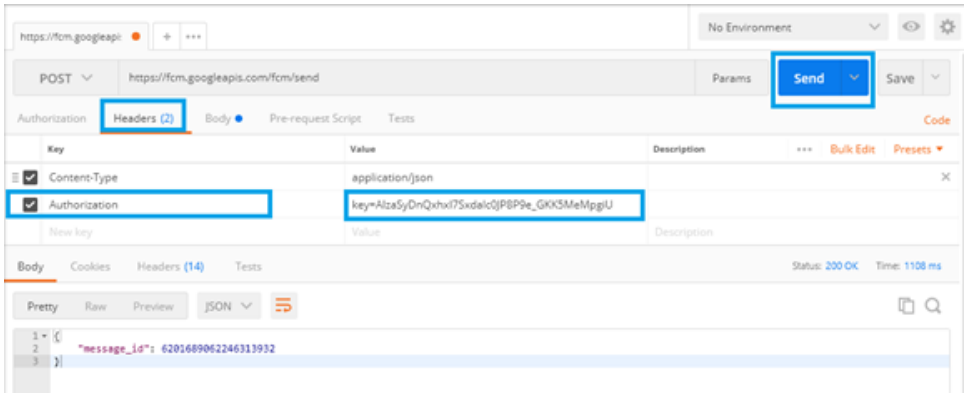
  "to":"/topics/Alerts"

  }

- Select the text to **Json**

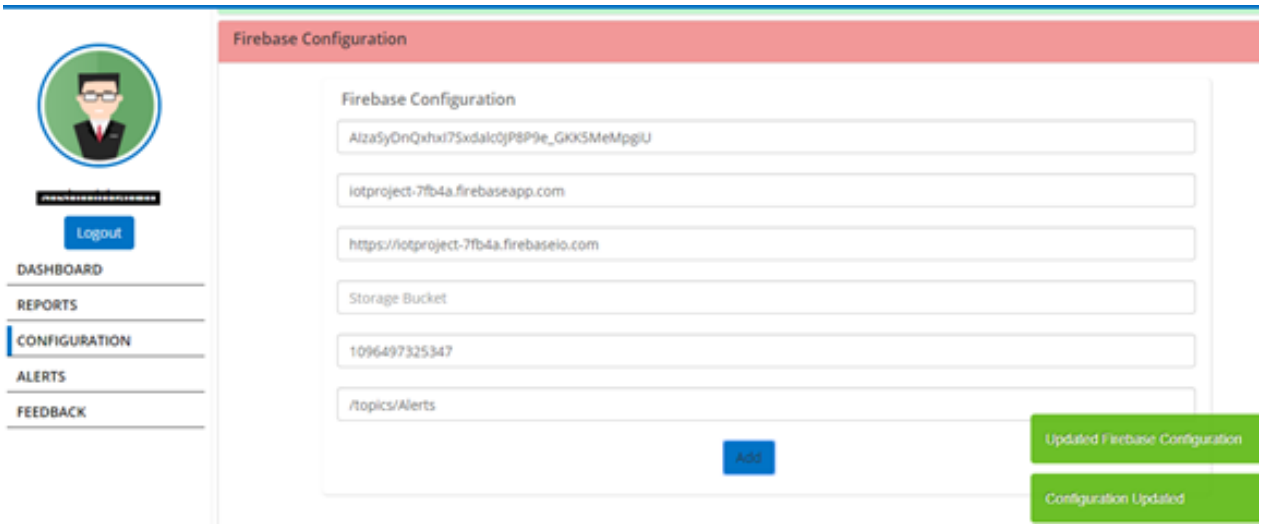


10. Click on **Headers**, add a new key called **Authorization** and give the value as **key=<Legacy Server Key>** which was obtained during step 5**.** Click on **Send.**



11. Paste the details in the respective tabs of **Firebase Configuration** after logging into Webapp and click on **Add**.

Note: For Messaging Reviewer Id, enter **/topics/Alerts**



14. Restore Virtual Machines

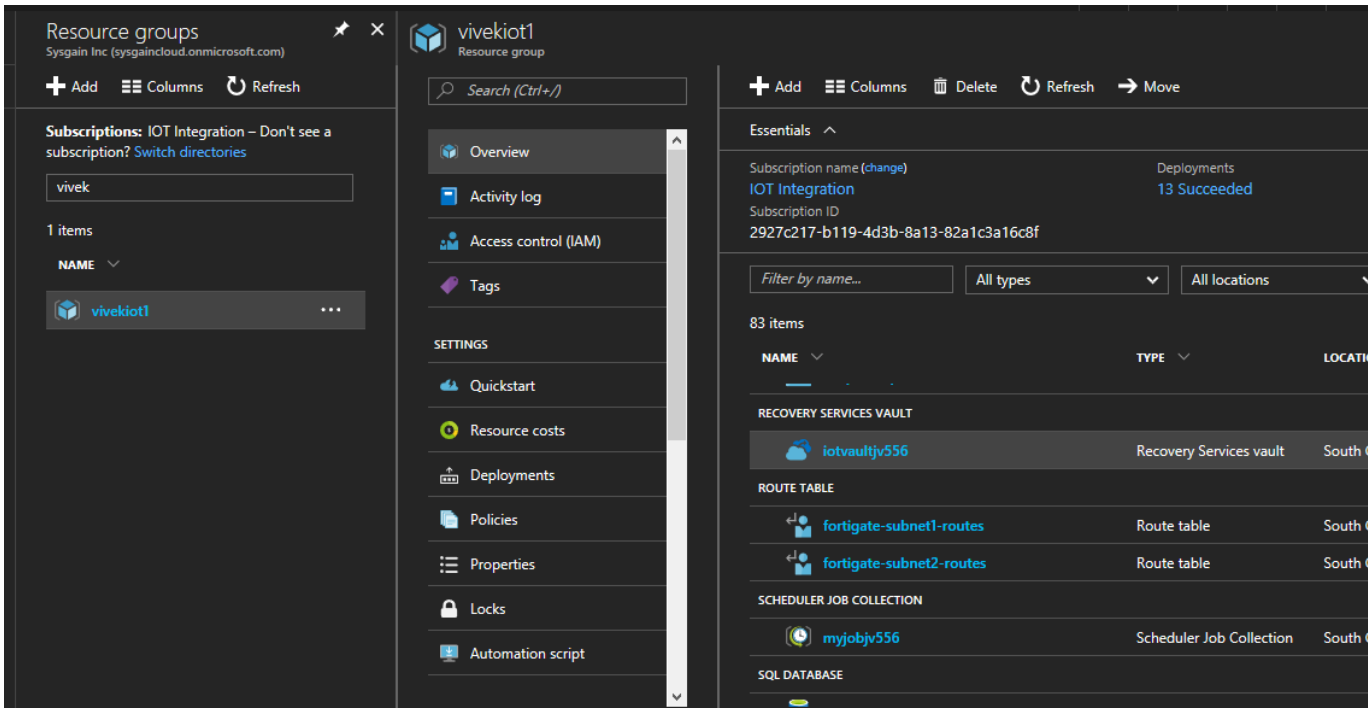
Protect your data by taking snapshots of your data at defined intervals. These snapshots are known as recovery points, and they are stored in recovery services vaults. If or when it is necessary to repair or rebuild a VM, you can restore the VM from any of the saved recovery points. When you restore a recovery point, you can create a new VM which is a point-in-time representation of your backed-up VM.

Restoring a VM or all disks from VM backup involves two steps:

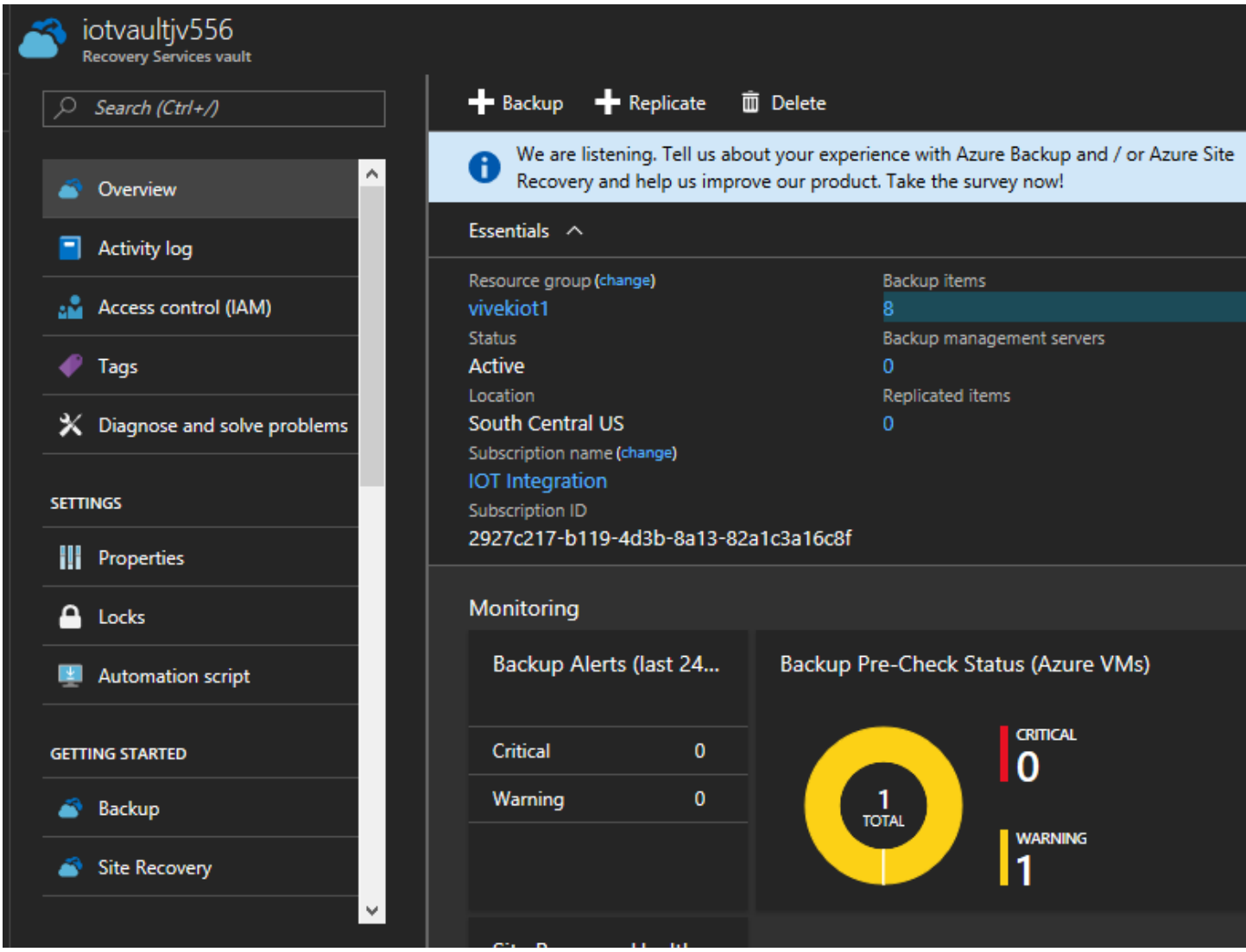
1. Select a restore point for restore
2. Selecting the restore type - create a new VM or restore disks and specify required parameters.

14.1. Select restore point for restore

1. Sign in to the Azure portal
2. Go to your Resource Group and from the resources list, select the vault associated with the VM's you want to restore.

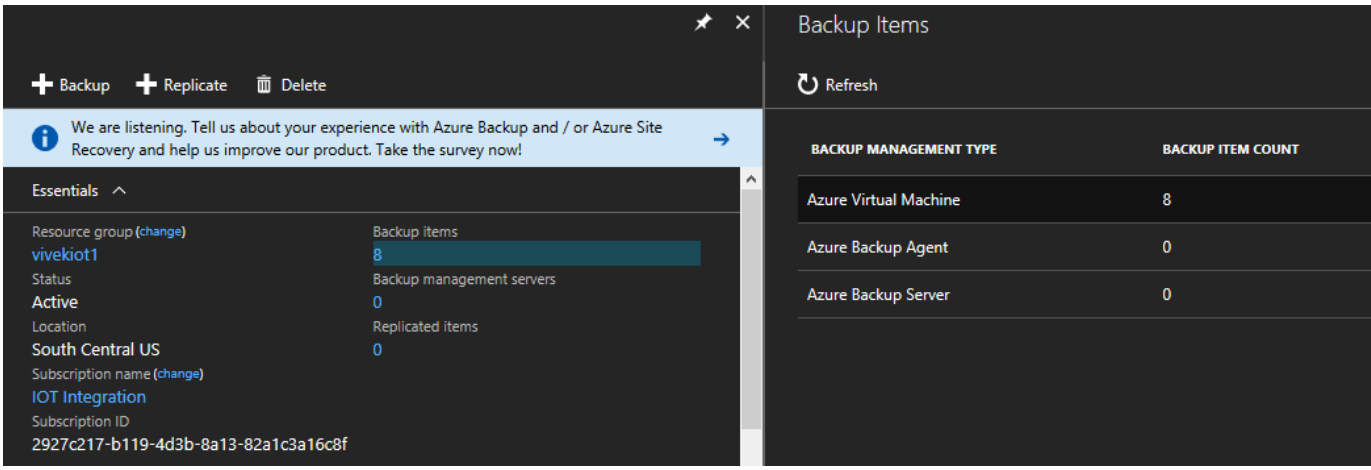


3. When you click the vault, its dashboard opens.

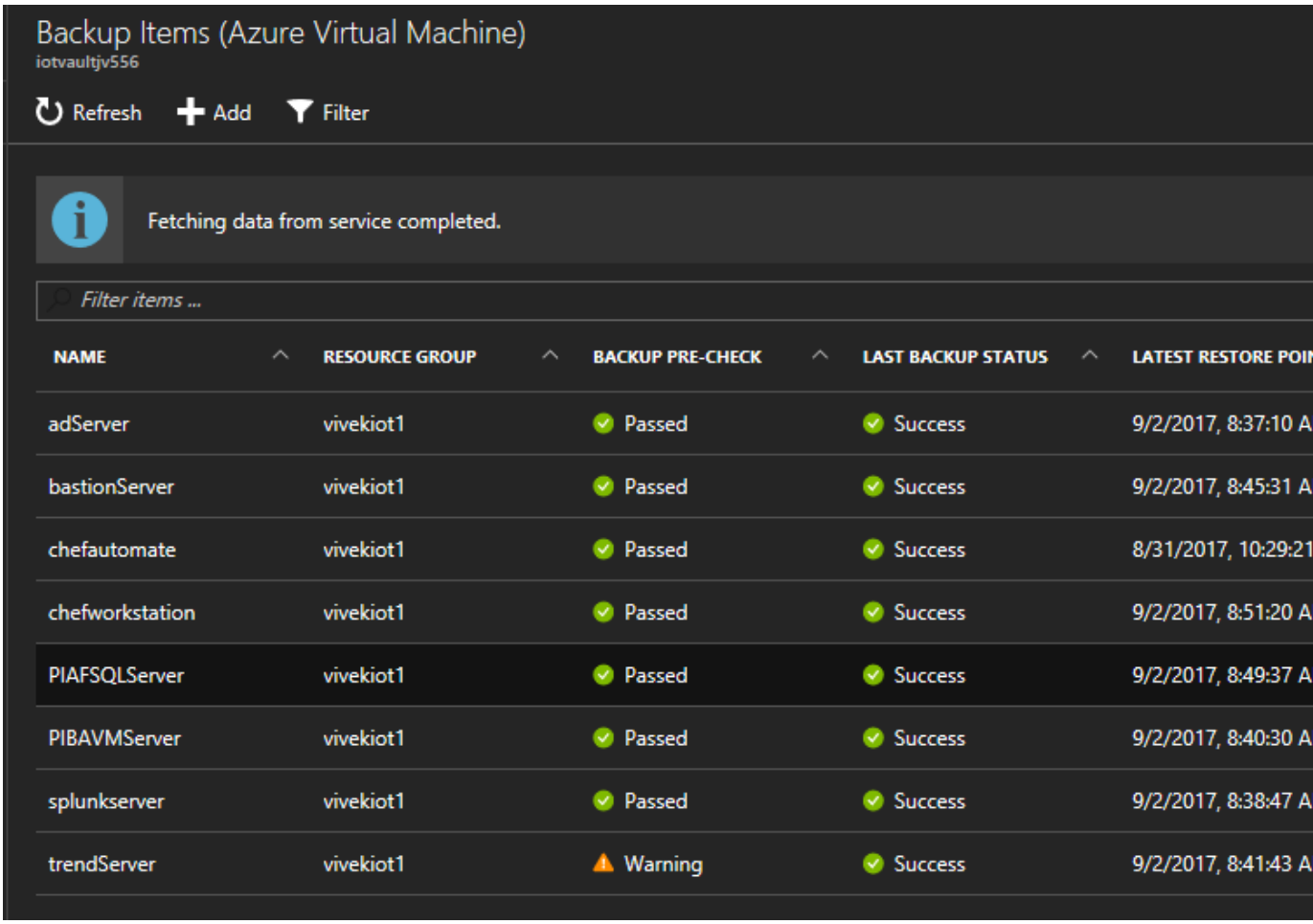


4. Now that you're in the vault dashboard. On the **Backup Items** tile, click **Azure Virtual Machines** to display the VMs associated with the vault.

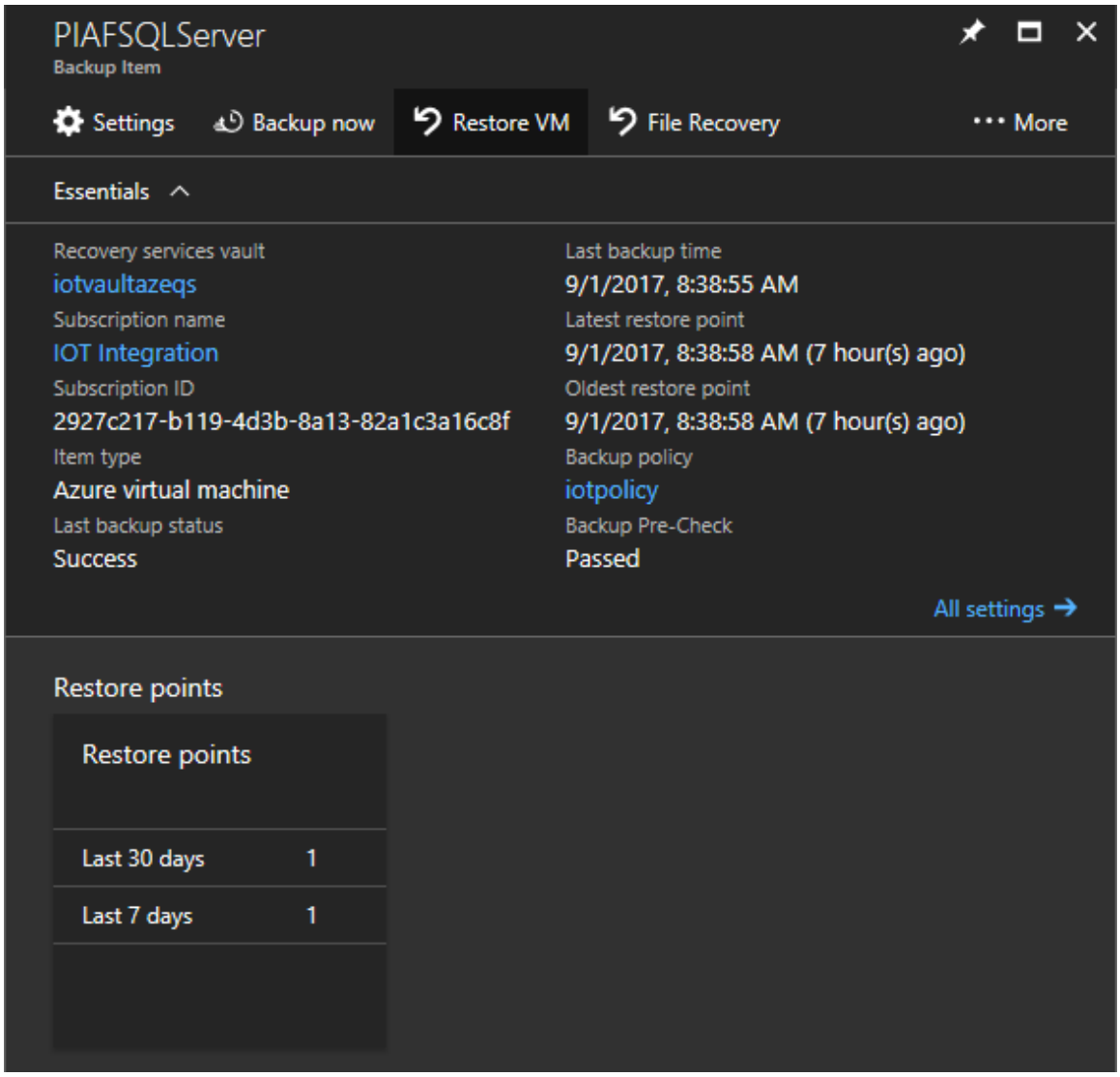
8



5. The **Backup Items** blade opens and displays the list of Azure virtual machines.



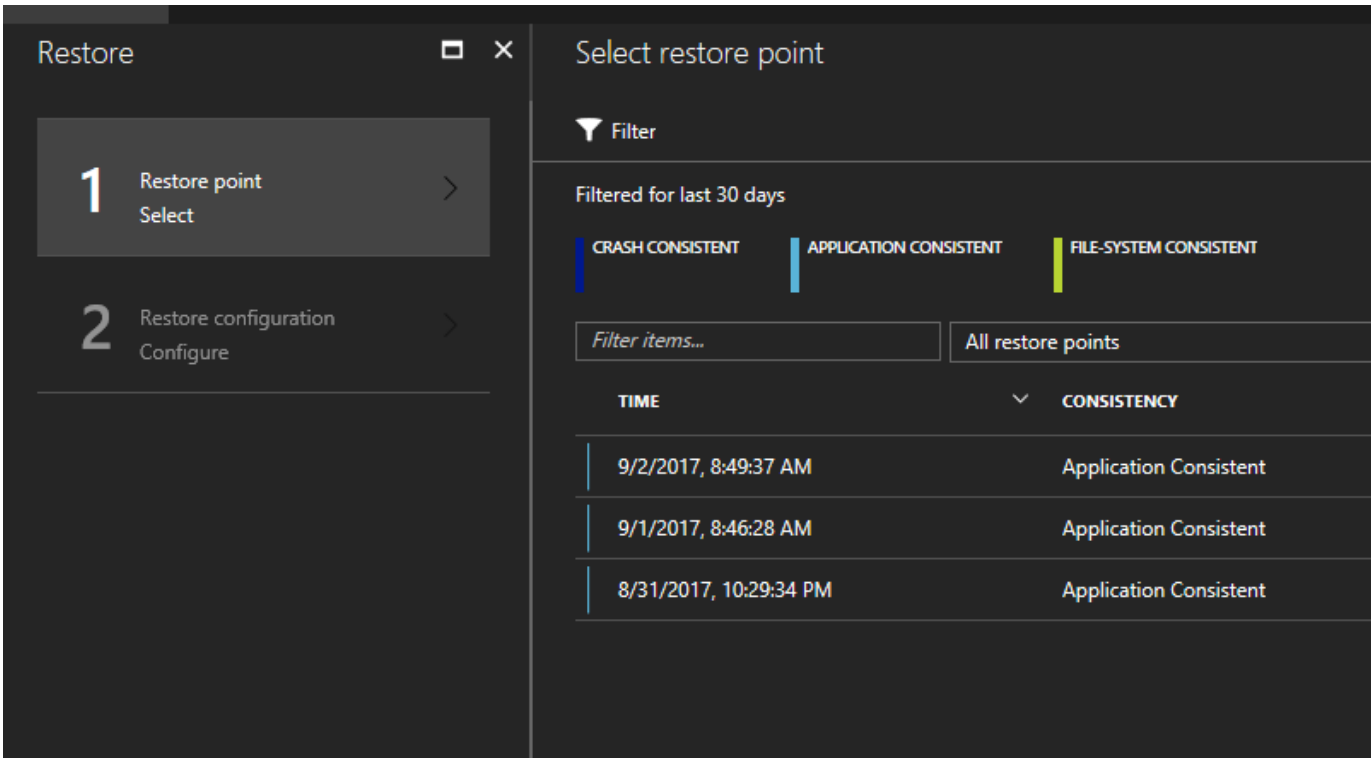
6. From the list, select a VM to open the dashboard. (ex : PIAFSQLServer) The VM dashboard opens to the Monitoring area, which contains the Restore points tile.



7. On the VM dashboard menu, click **Restore**

   The Restore blade opens.

8. On the **Restore** blade, click **Restore point** to open the **Select Restore point** blade.

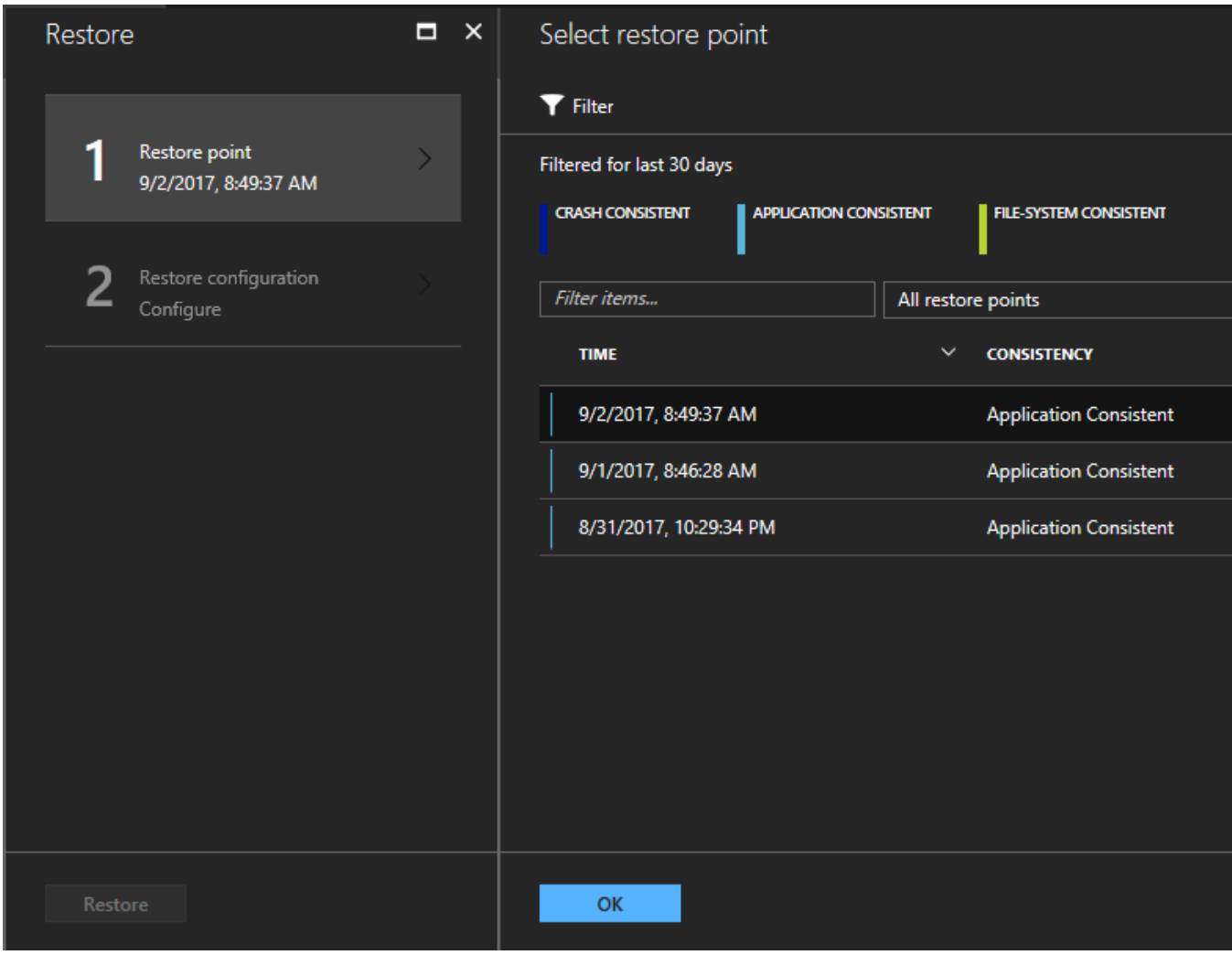


9. By default, the dialog displays all restore points from the previous days. Use the **Filter** to alter the time range of the restore points displayed. By default, restore points of all consistency are displayed.

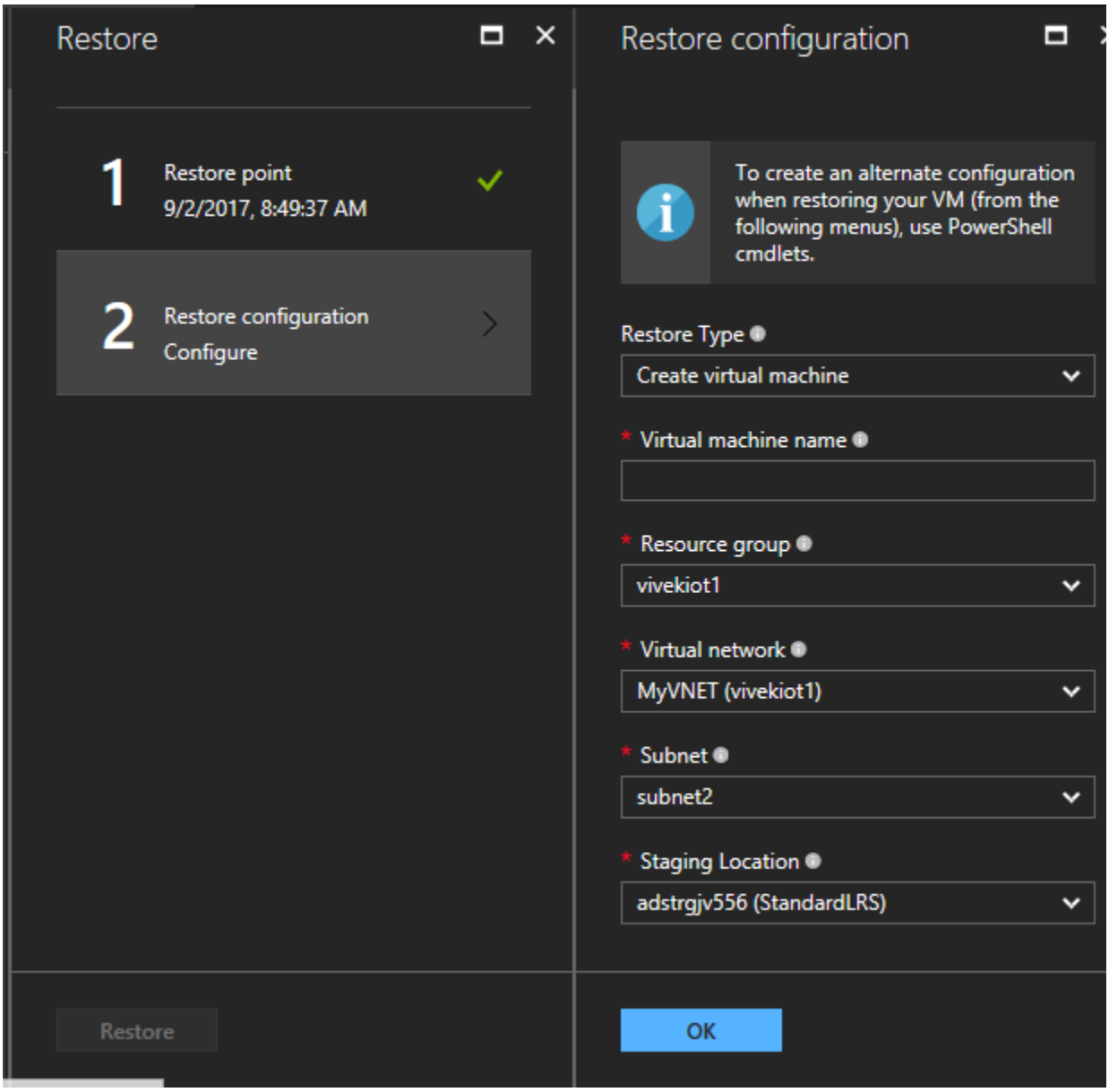
   Restore point consistency from this list choose:

   - Crash consistent restore points,
   - Application consistent restore points,
   - File system consistent restore points
   - All restore points.

10. Choose a Restore point and click OK.



11. The Restore blade shows the Restore point is set.
12. On the Restore blade, Restore configuration opens automatically after restore point is set.



14.2. Choosing a VM restore configuration

1. Now that you have selected the restore point, choose a configuration for your restore VM.
2. On the Restore configuration blade, you have two choices:

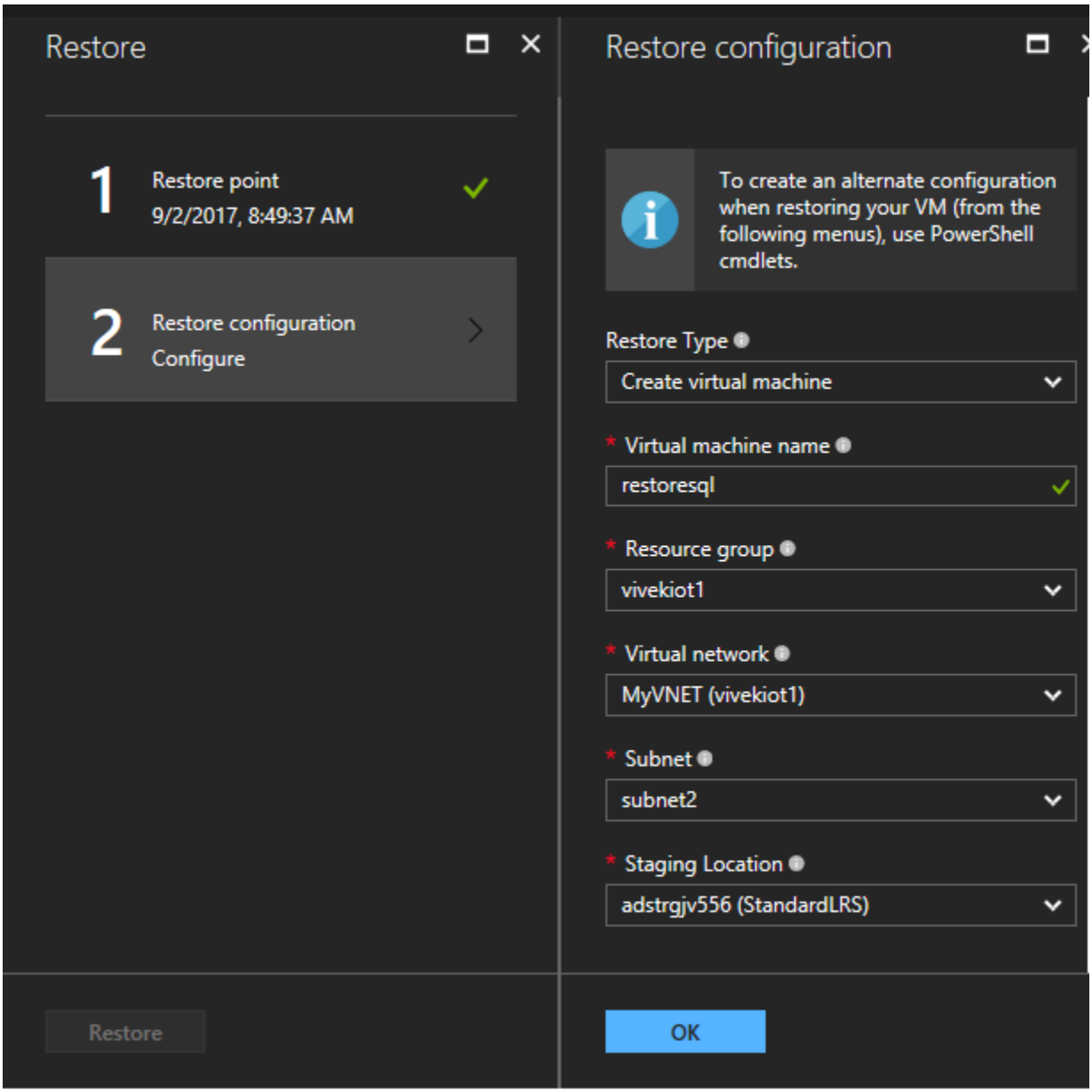
- Restore full virtual machine
- Restore backed up disks

14.2.1. Create a new VM from restore point

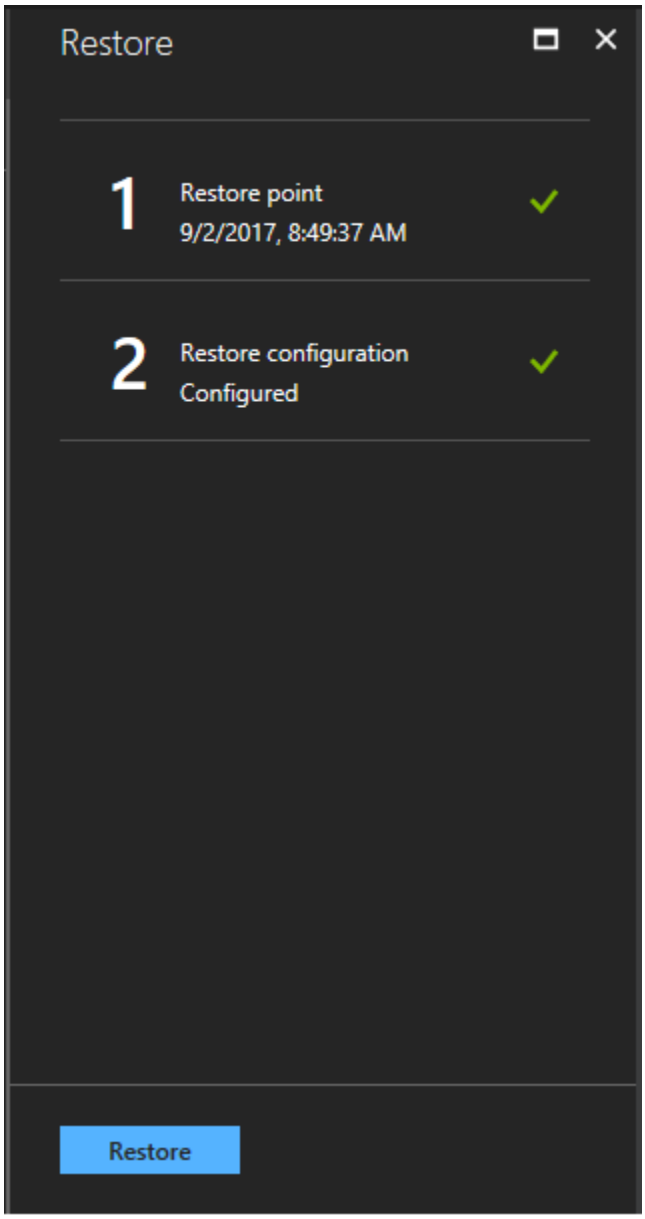
Select Restore Type as Create virtual machine.

Once restore point is selected, on the Restore configuration blade, enter or select values for each of the following fields:

1. **Restore Type** - Create virtual machine.
2. **Virtual machine name** - Provide a name for the VM. The name must be unique to the resource group (for a Resource Manager-deployed VM) or cloud service (for a Classic VM). You cannot replace the virtual machine if it already exists in the subscription.
3. **Resource group** - Use an existing resource group, or create a new one.
4. **Virtual Network** - Select the virtual network (VNET) when creating the VM. The field provides all VNETs associated with the subscription. Resource group of the VM is displayed in parentheses.
5. **Subnet** - If the VNET has subnets, the first subnet is selected by default. If there are additional subnets, select the desired subnet.
6. **Storage account** - This menu lists the storage accounts in the same location as the Recovery Services vault. Storage accounts that are Zone redundant are not supported. If there are no storage accounts with the same location as the Recovery Services vault, you must create one before starting the restore operation. The storage account's replication type is mentioned in parentheses.

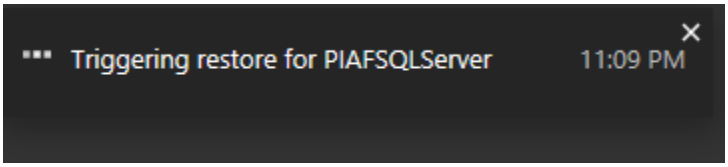


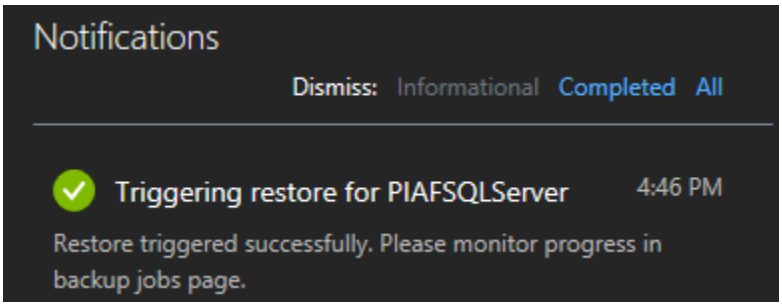
7. On the **Restore configuration** blade, click **OK** to finalize the restore configuration.
8. On the **Restore** blade, click **Restore** to trigger the restore operation.



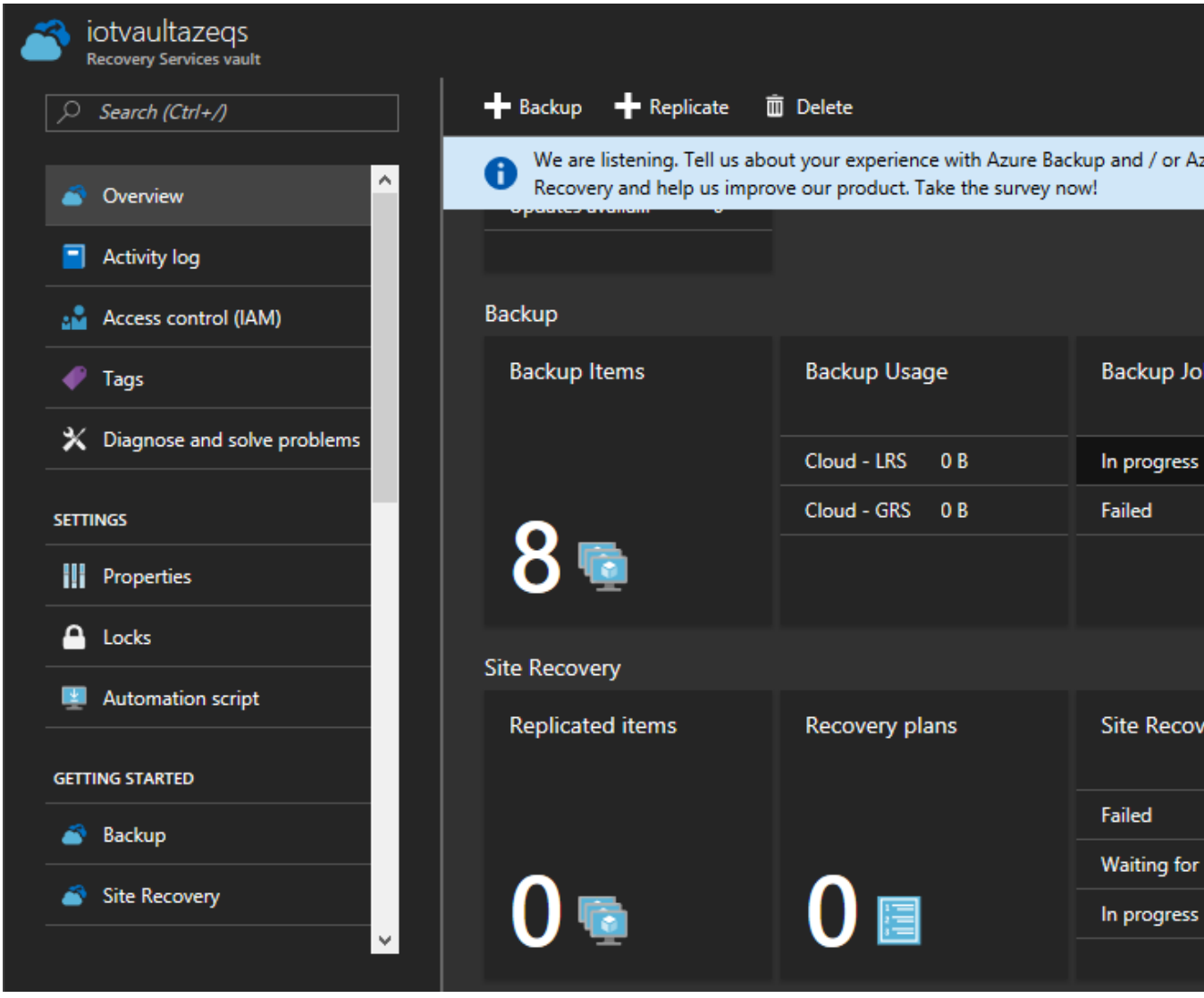
14.3. Track the restore operation

1. Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation.



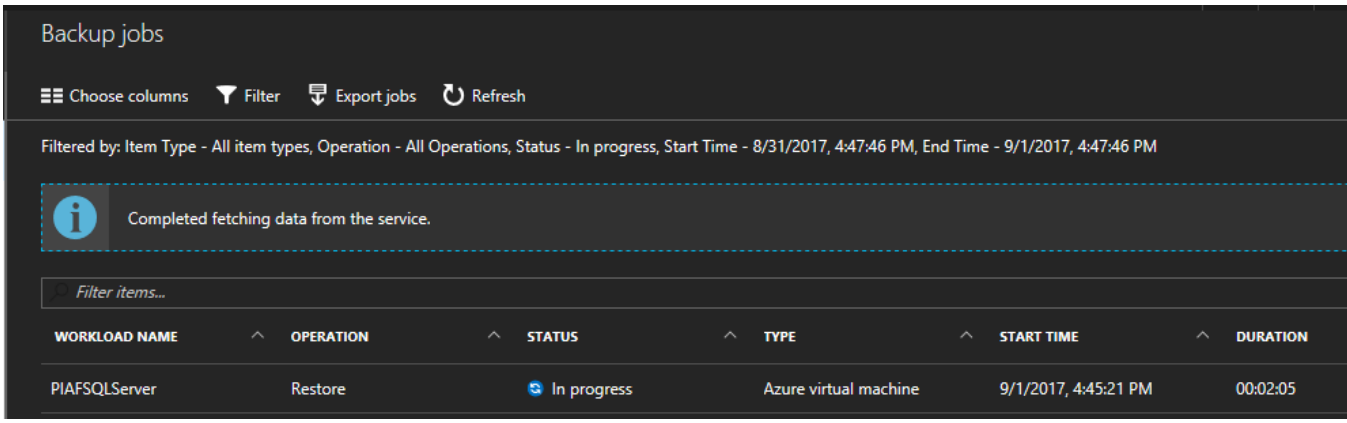


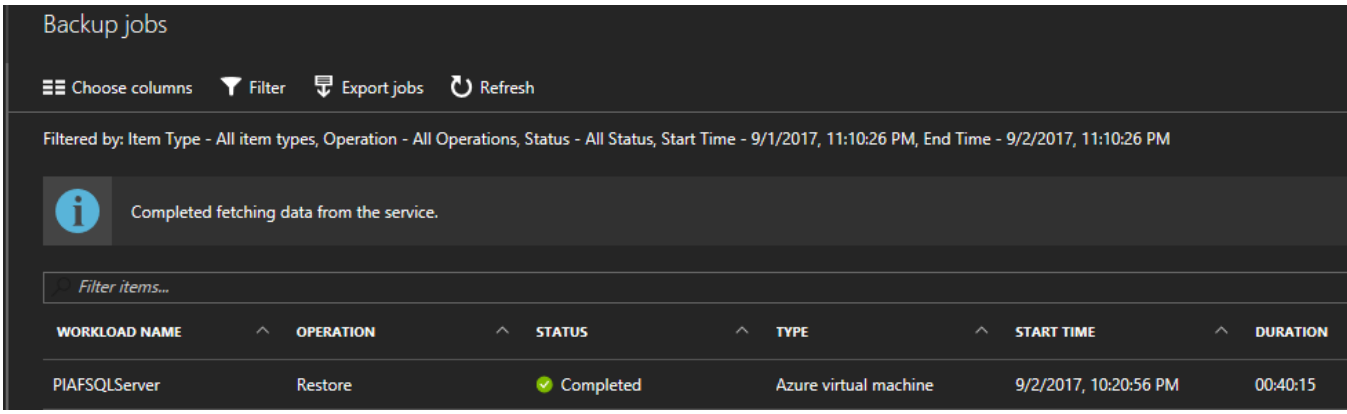
2. To view the operation while it is processing, or to view when it completed, open the Backup jobs list.
3. In the vault dashboard on the **Backup Jobs** tile, click **Azure Virtual Machines** to display the jobs associated with the vault.



4. The **Backup Jobs** blade opens and displays the list of jobs.

8

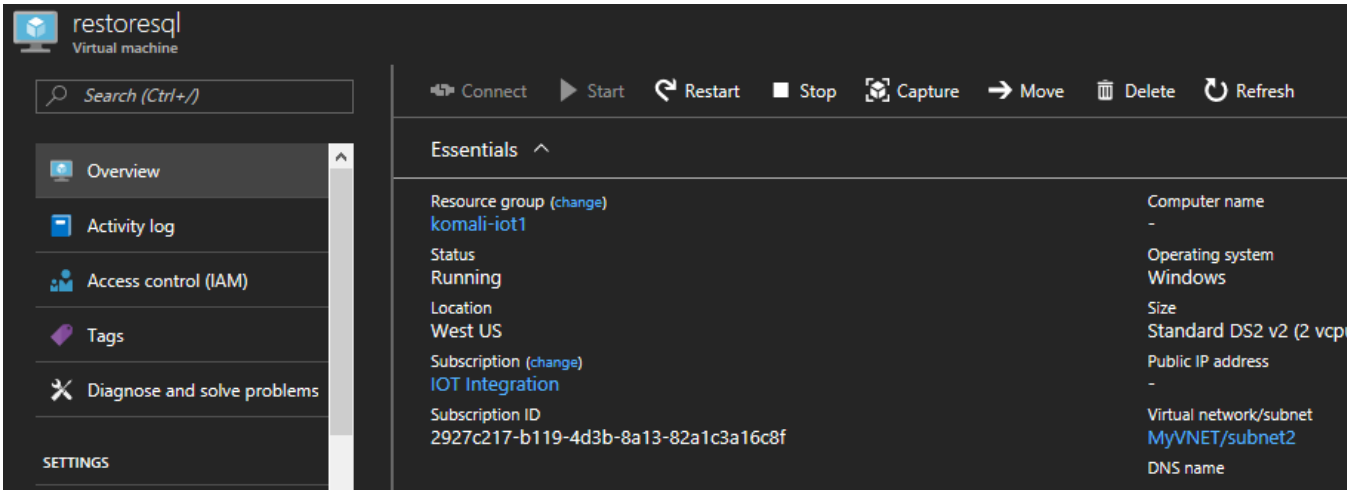




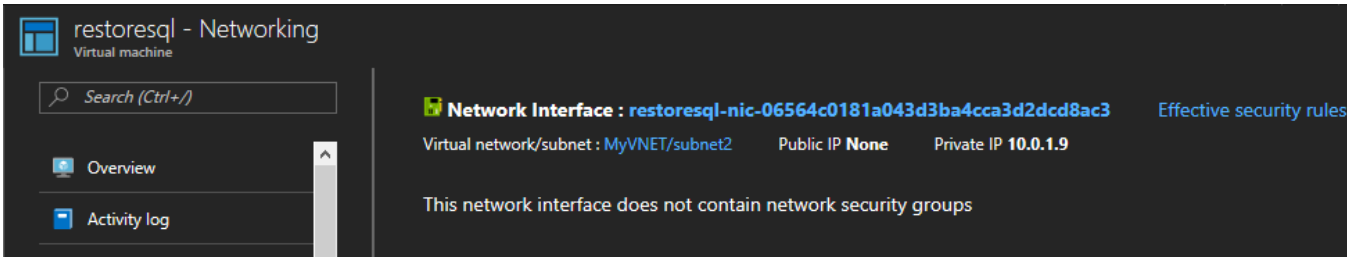
5. Once the restoration is completed, go to the resource group in where you have created the new restored VM.

Post-Restore steps

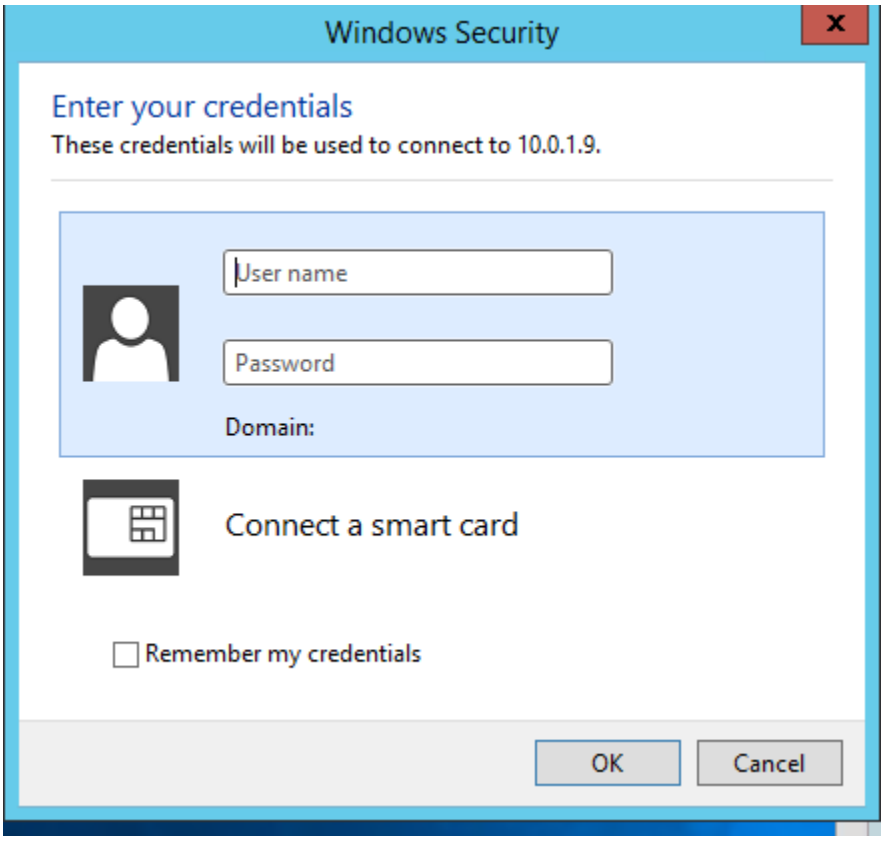
1. If the backed-up VM has static IP, post restore, restored VM will have a dynamic IP to avoid conflict when creating restored VM.



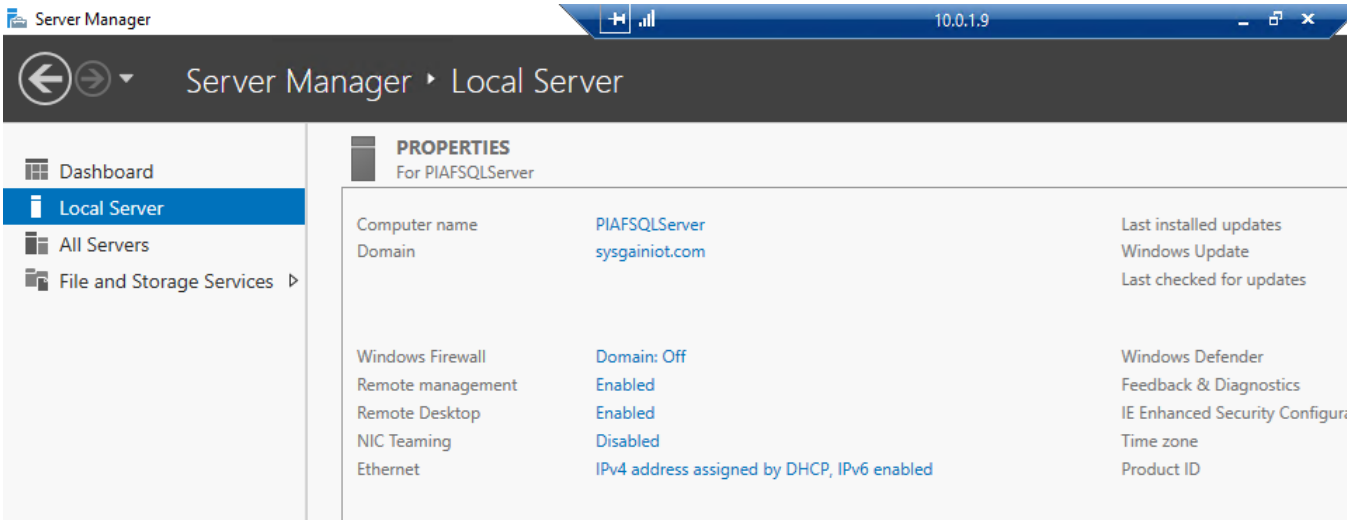
2. Login to that VM using its newly created IP.

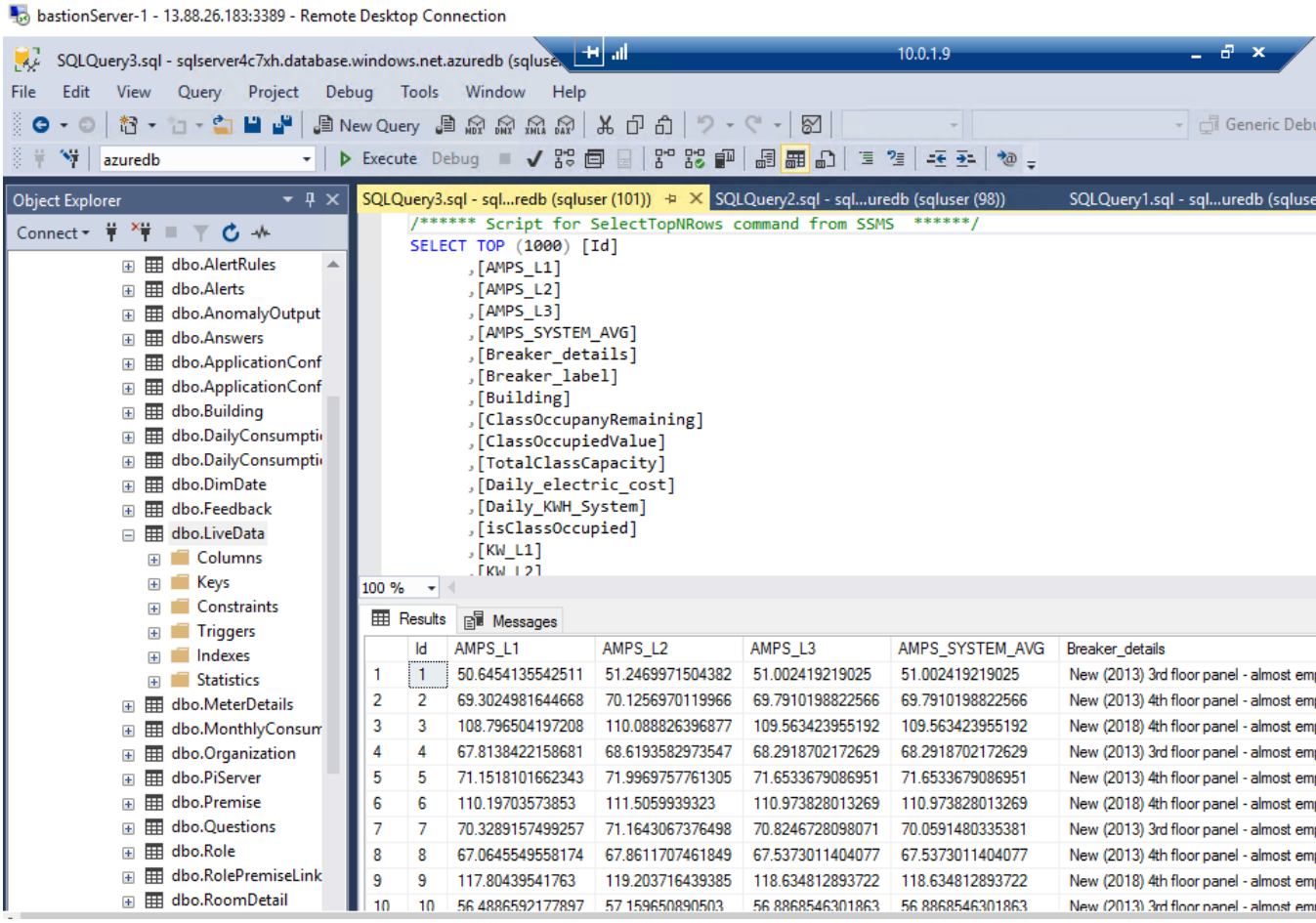


3. And check whether it has all the restored data or not.


Windows Security
Enter your credentials
These credentials will be used to connect to 10.0.1.9.
User name
Password
Domain:
Connect a smart card
Remember my credentials
OK
Cancel

8


Server Manager
10.0.1.9
Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For PIAFSQLServer
Computer name
PIAFSQLServer
Domain
sysgainiot.com
Last installed updates
Windows Update
Last checked for updates
Windows Firewall
Domain: Off
Remote management
Enabled
Remote Desktop
Enabled
NIC Teaming
Disabled
Ethernet
IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender
Feedback & Diagnostics
IE Enhanced Security Configura
Time zone
Product ID



4. If you are using a cloud-init based Linux distribution such as Ubuntu, for security reasons, password is blocked post restore. Please use VMAccess extension on the restored VM to reset the password.

Backup for restored VMs

If you have restored VM to same Resource Group with the same name as originally backed up VM, backup continues on the VM post restore. If you have either restored VM to a different Resource group or specified a different name for restored VM, this is treated as a new VM and you need to setup backup for restored VM.