



Internet of Things Automation

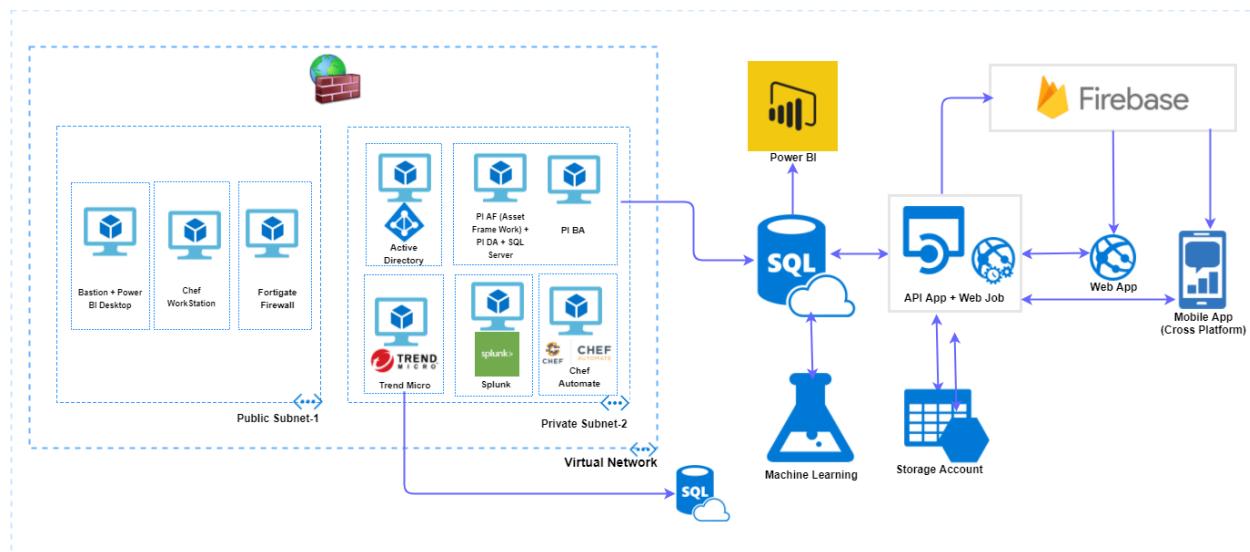
User Guide

Contents

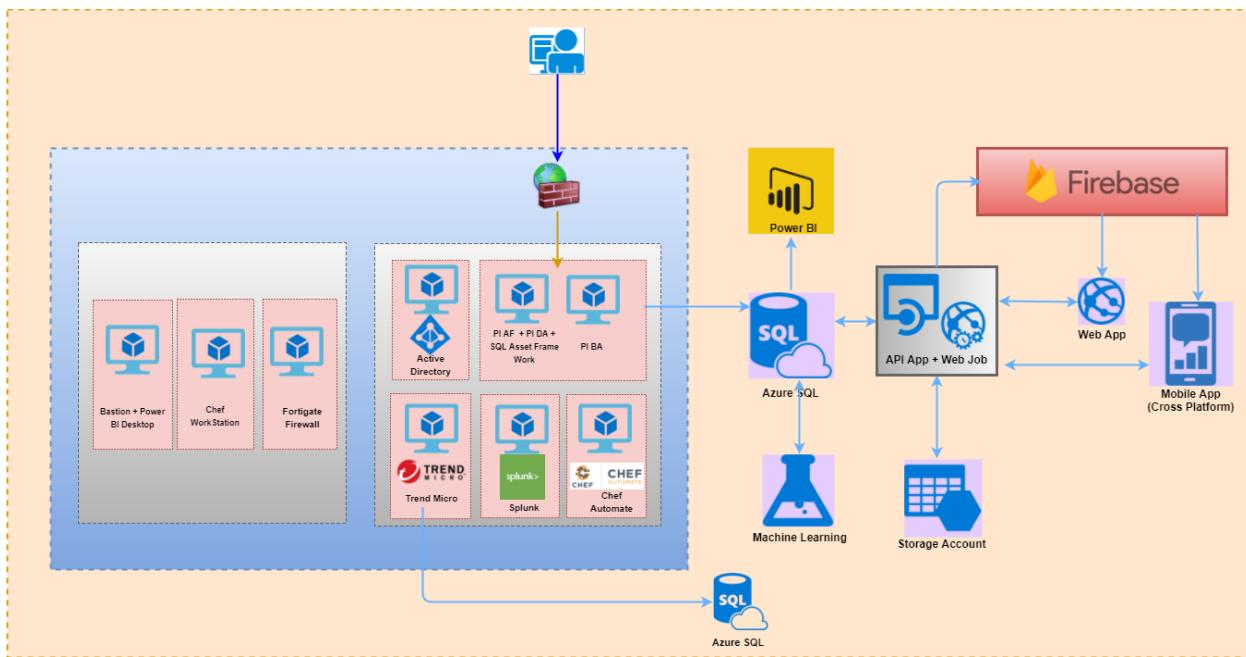
1.	Architecture	4
1.1.	Data Flow Architecture Diagram.....	5
2.	High Level Deployment Process to be Followed.....	5
3.	Deployment Costs	6
3.1.	SERVER DETAILS	7
4.	Prerequisites.....	8
4.1	Launching Firewall Template	8
4.2.	Azure B2C Tenant Creation and Configuration	21
4.3.	Power BI Configuration.....	40
4.4.	Dynatrace Account Creation (If You Don't Have an Existing Account)	46
5.	Input Parameters	50
6.	Azure Resource Manager Template Deployment	53
6.1.	Output Parameters.....	58
7.	Security and Monitoring Components.....	61
7.1.	Dynatrace.....	62
7.1.1.	Installing Dynatraceoneagent To Web Application (PaaS Environment)	73
7.2.	Chef Automate.....	84
7.3.	Splunk.....	88
7.4.	TrendMicro	90
8.	Create User for PI Business Analytics (PIBA) Interface	105
8.1.	Create PIBA User in PIAF Server	115
8.2.	Enable TCP and Named Pipe in SQL Server Configuration Management.....	122
9.	Components of PI Server.....	125
9.1.	PI Asset FrameWork (AF)	125
9.1.1.	Installation of PIAF Server	126
9.2.	PI Data Archive (PIDA).....	128
9.2.1.	Installation of Data Archive (PIDA)	129

9.3. PI Web API Utility	139
9.4. Creation of Database in PI System Explorer	145
9.5. System Configuration in PI System Explorer	148
9.6. Import .XML Files into AF Server	152
9.7. Update Security in PI System Management Tools	160
9.8. Prepare Data Server for Module Database(MDB) To Asset Framework(AF).....	174
9.9. Update PI Points in PI System Explorer.....	178
9.10. Install and Run The Piweb Simulator Setup.....	182
10. Installation of PI BA Integrator.....	189
10.1. Configuring PI Business Analytics.....	196
10.2. Install And Run The DataServiceAppSetup	214
11. Configuring and Accessing the Webapp.....	239
12. Machine Learning Experiment	244
13. Firebase Configuration.....	256
14. Restore Virtual Machines.....	262
14.1. Select restore point for restore	262
14.2. Choosing a VM restore configuration	269
14.2.1. Create a new VM from restore point.....	270
14.3. Track the restore operation.....	272

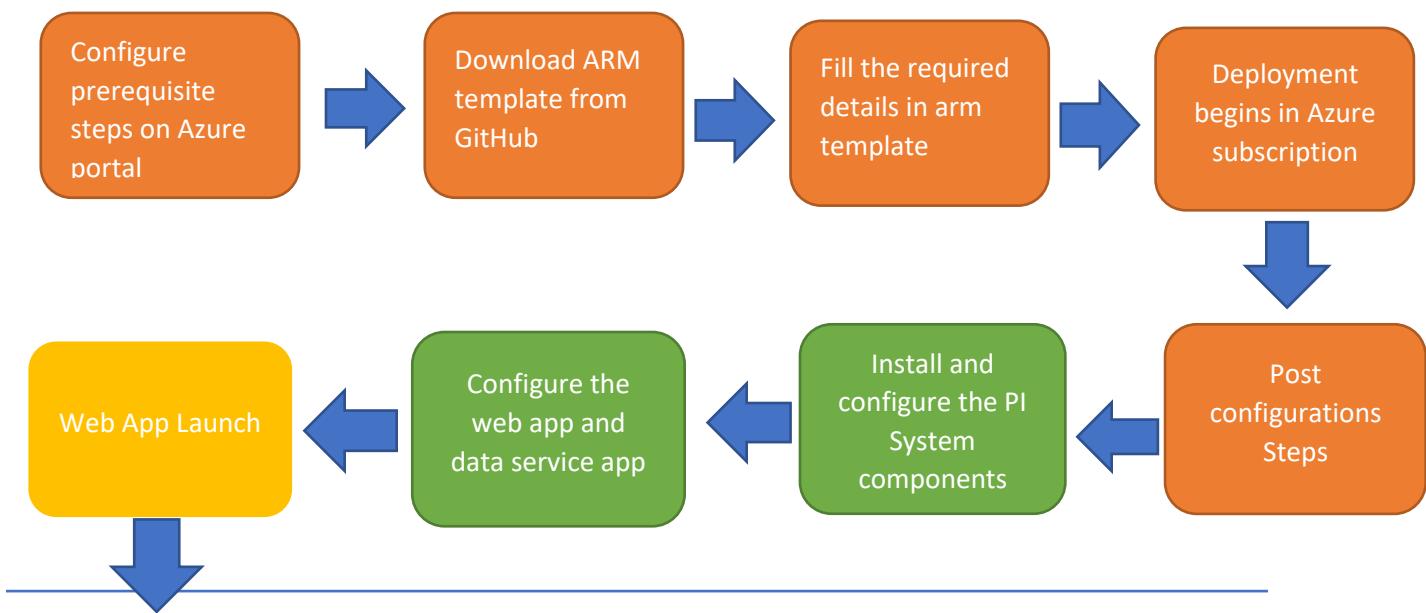
1. Architecture



1.1. Data Flow Architecture Diagram



2. High Level Deployment Process to be Followed



Configure
services & see
data on web app

- Prerequisites
- core components
- configurations

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**.

Microsoft Azure New > Template deployment

Template deployment Microsoft

Applications running in Microsoft Azure usually rely on a combination of resources, like databases, servers, and web apps. Azure Resource Manager templates enable you to deploy and manage these resources as a group, using a JSON description of the resources and their deployment settings.

Edit your template with IntelliSense and deploy it to a new or existing resource group.

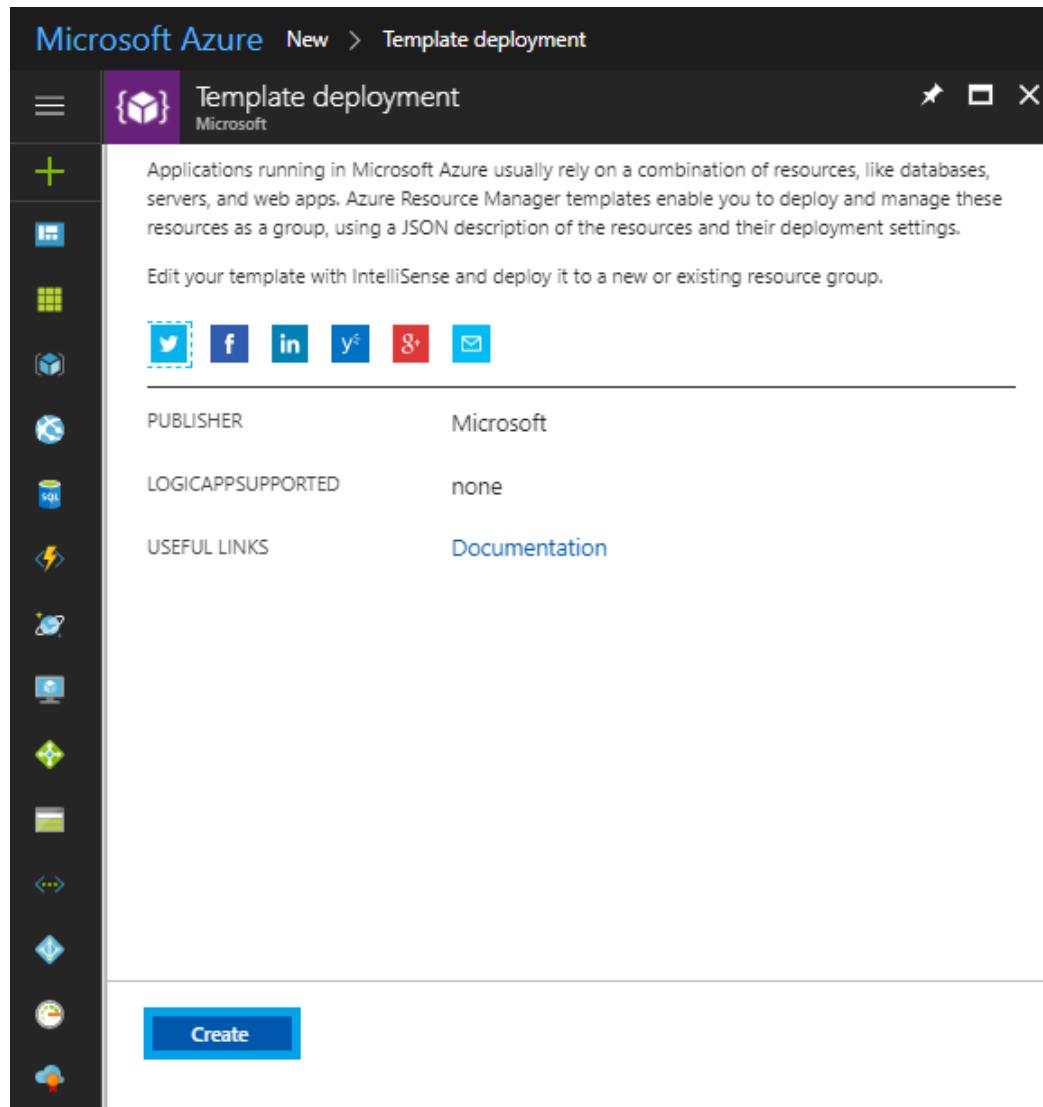
[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)

PUBLISHER Microsoft

LOGICAPPSSUPPORTED none

USEFUL LINKS [Documentation](#)

[Create](#)



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

Custom deployment
Deploy from a custom template

Learn about template deployment

[Read the docs](#)

[Build your own template in the editor](#)

Common templates

[Create a Linux virtual machine](#)

[Create a Windows virtual machine](#)

[Create a web app](#)

[Create a SQL database](#)

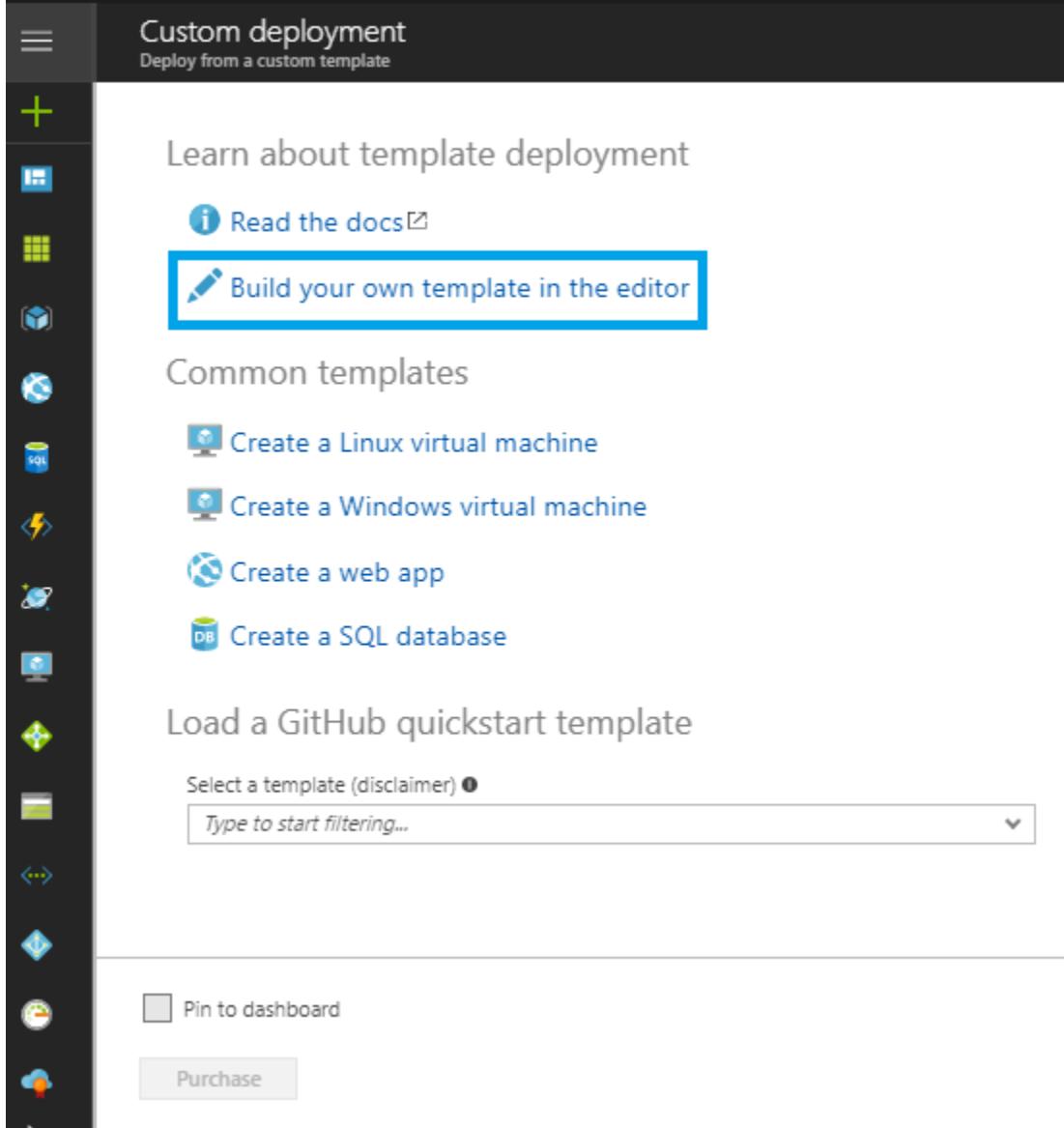
Load a GitHub quickstart template

Select a template (disclaimer) [●](#)

Type to start filtering...

Pin to dashboard

Purchase



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



[Edit template](#)

Edit template

 Add resource Quickstart template Load file Download

►  Parameters (3)

▶ Variables (9)

▼ Resources (4)

 [variables('fortigateFirewallSetting...]

Variables('fortigateFirewallSetting...')

```
<--> [variables('networkSettings')].virtual...
```

 fortigateServer (Microsoft Resource)

```
1 {
2     "$schema": "https://schema.management.azure.com/schemas/2015-01-01/c
3     "contentVersion": "1.0.0.0",
4     "parameters": {
5         "adminUsername": {
6             "type": "string",
7             "defaultValue": "",
8             "metadata": {
9                 "description": "Username for fortigate Virtual Machine,
10                }
11            },
12            "adminPassword": {
13                "type": "securestring",
14                "defaultValue": "",
15                "metadata": {
16                    "description": "Password for fortigate Virtual Machine,
17                    }
18                },
19                "fortigateVMSize": {
20                    "type": "string",
21                    "defaultValue": "Standard_D2_v2",
22                    "allowedValues": [
23                        "Standard_D1_v2",
24                        "Standard_D2_v2",
25                        "Standard_D3_v2"
26                    ]
27                }
28            }
29        }
30    }
31 }
```

Save

Discard

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

This template, prices and associated legal terms for any marketplace offerings can be found in the [Azure Marketplace](#), but may be 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

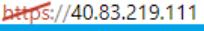
6. After deploying the template, go to the Fortigate Virtual Machine resource in the Resource Group. Click on that resource, then copy the IP address.

Connect Start Restart Stop Capture Move Delete Refresh

Essentials ^

Resource group (change) fortigate-test	Computer name fortigate
Status Running	Operating system Linux
Location West US	Size Standard D2 v2 (2 vcpus, 7 GB memory)
Subscription (change) 	Public IP address 40.83.219.111
Subscription ID 	Virtual network/subnet MyVNET/PublicFacingSubnet
	DNS name fortigatekeokf.westus.cloudapp.azure.com

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

 Not secure 

System Dashboard - Microsoft Office Home Mail - sushmithan@ Dashboard - Microsoft

Your connection is not private

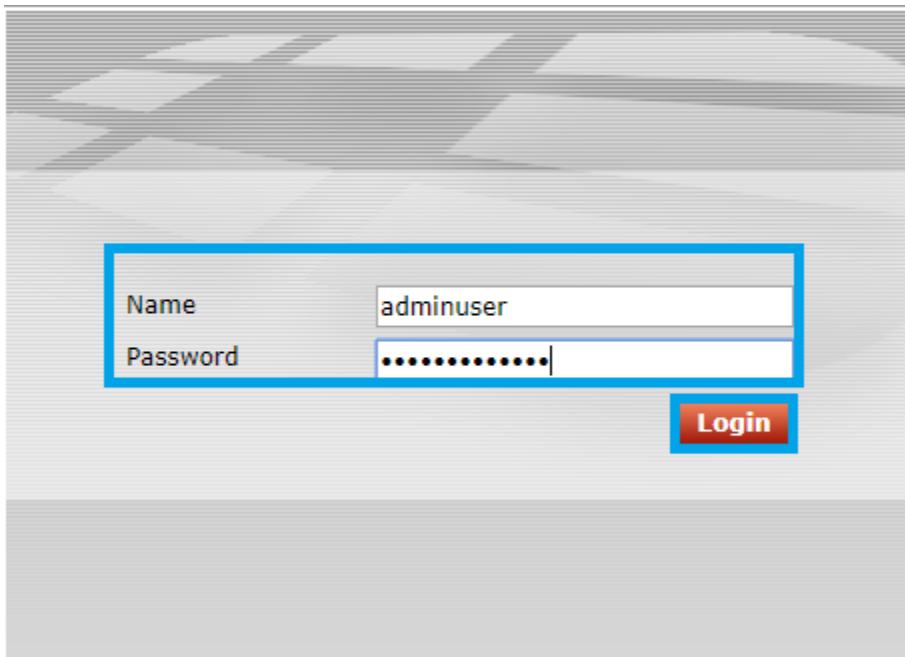
Attackers might be trying to steal your information from **40.83.219.111** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

[ADVANCED](#) [Back to safety](#)

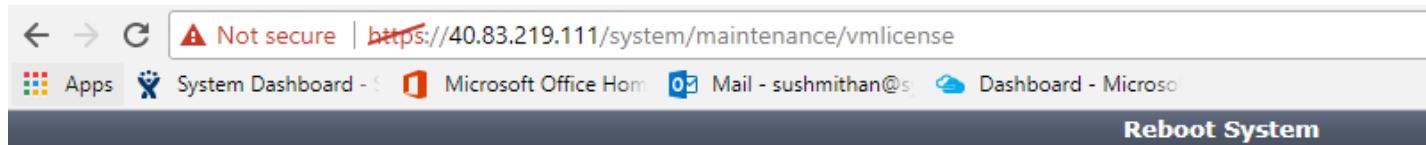
8. The login popup box will appear. Give the admin username and admin password that you provided in the parameter section. Then click on Login.



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.

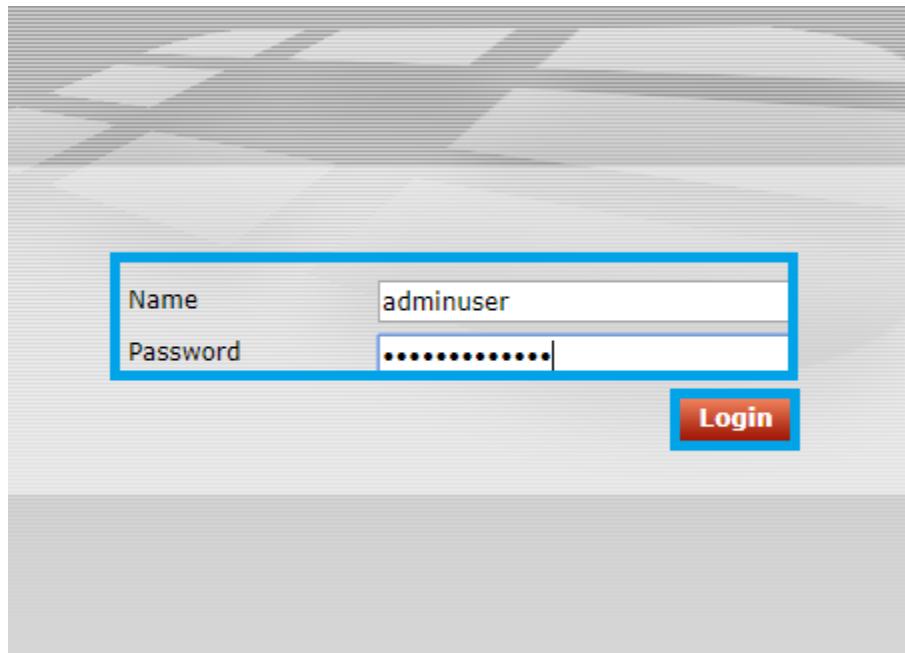


10. After this, the system will automatically restart. It may take up to 15 minutes.



Please wait while system restarts.

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.

System

-  [Dashboard](#)
-  **Status**
-  [FortiView](#)
-  [Network](#)
-  [Config](#)
-  [Admin](#)
-  [Certificates](#)
-  [Monitor](#)

Router

- [Policy & Objects](#)
- [Security Profiles](#)
- [VPN](#)
- [User & Device](#)
- [WiFi Controller](#)
- [Log & Report](#)

 Widget
 Dashboard

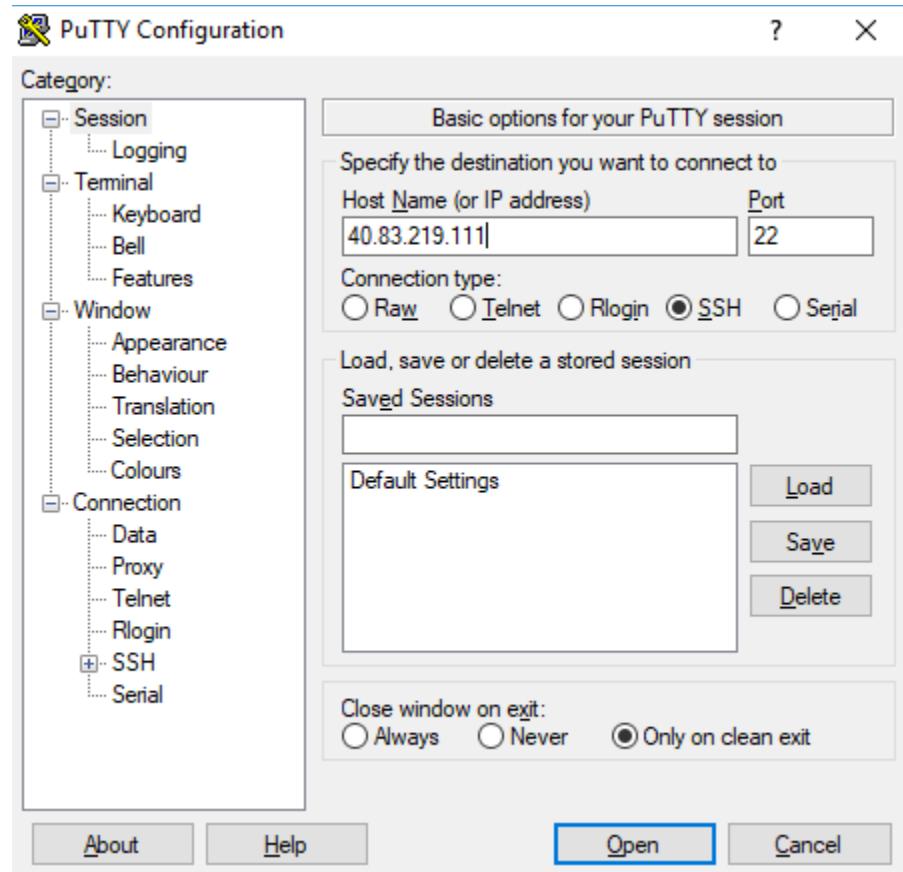
System Information

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)

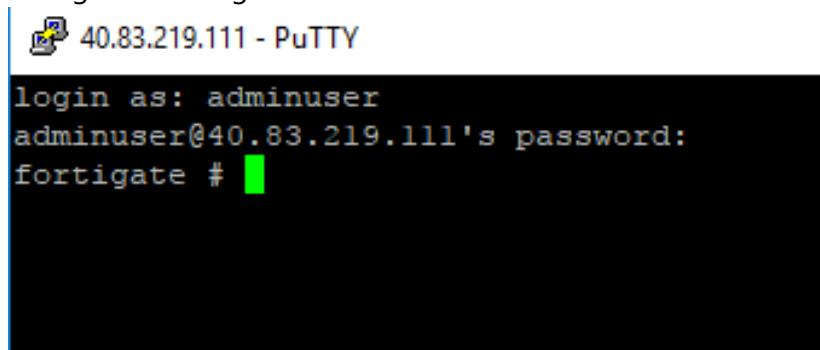
License Information

 Virtual Machine	<ul style="list-style-type: none"> • License Valid • CPUs 2 of 2
 Support Contract	<ul style="list-style-type: none"> • Registration Registered (mchandra@sysgain.com)
 FortiGuard	<ul style="list-style-type: none"> • IPS & Application Control Licensed (Expires 2017-10-31) • AntiVirus Licensed (Expires 2017-10-31) • Web Filtering Unreachable
 FortiCloud	<ul style="list-style-type: none"> • Account
 FortiSandbox	<ul style="list-style-type: none"> • FortiSandbox Appliance Not Configured
 FortiClient	<ul style="list-style-type: none"> • Clients Registered 0 of 10 • FortiClient Installers

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.



```
40.83.219.111 - PuTTY
login as: adminuser
adminuser@40.83.219.111's password:
fortigate #
```

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.

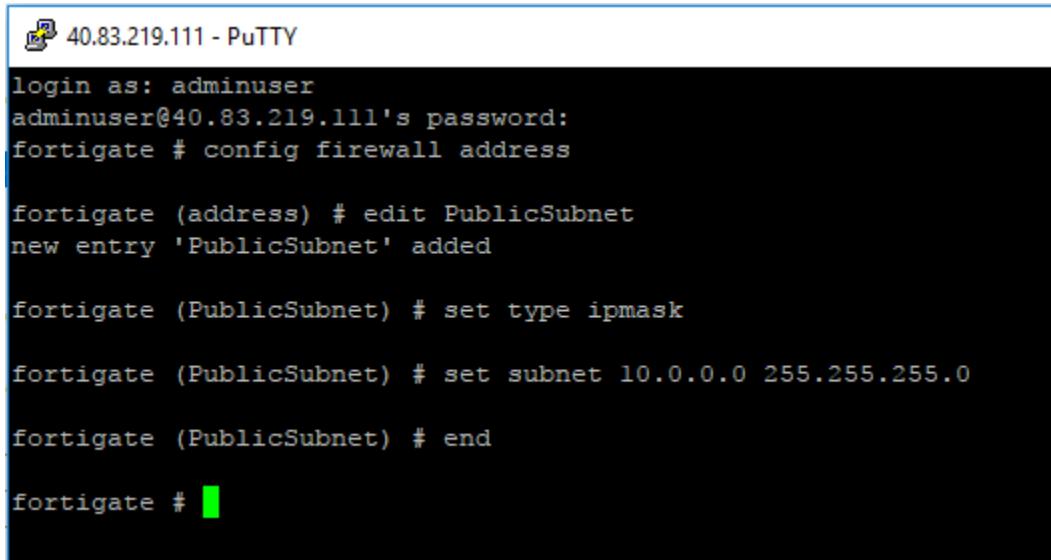
config firewall address

edit PublicSubnet

set type ipmask

set subnet 10.0.0.0 255.255.255.0

end



```

40.83.219.111 - PuTTY
login as: adminuser
adminuser@40.83.219.111's password:
fortigate # config firewall address

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

fortigate (PublicSubnet) # set type ipmask

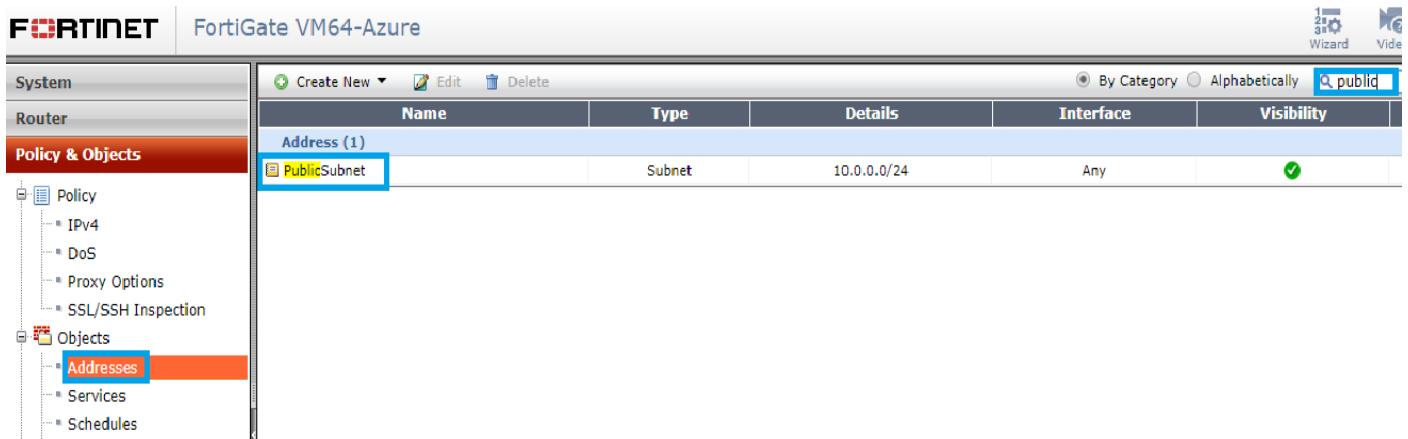
fortigate (PublicSubnet) # set subnet 10.0.0.0 255.255.255.0

fortigate (PublicSubnet) # end

fortigate #

```

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.



Name	Type	Details	Interface	Visibility
PublicSubnet	Subnet	10.0.0.0/24	Any	✓

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

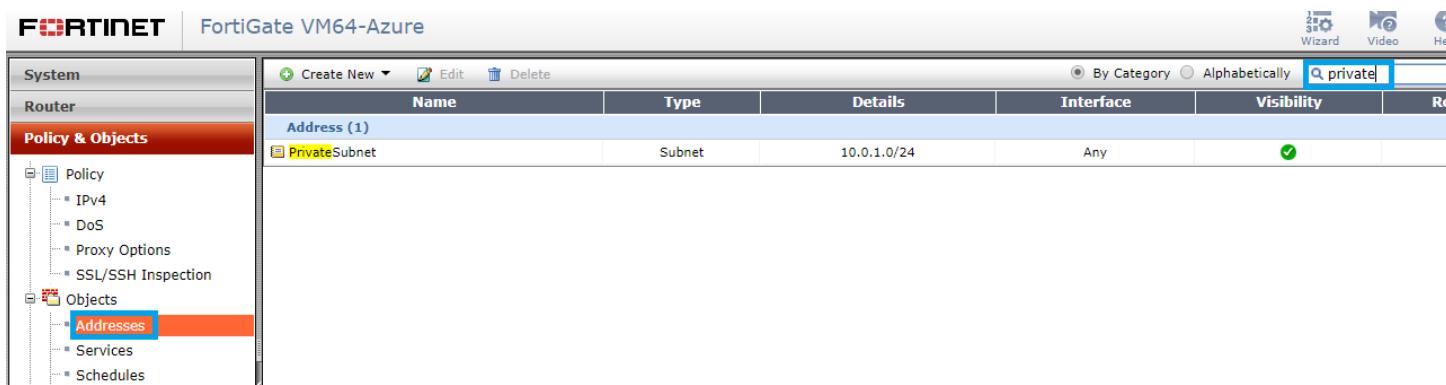
fortigate (PrivateSubnet) # set subnet 10.0.1.0 255.255.255.0

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.



The screenshot shows the Fortinet FortiGate VM64-Azure interface. The left sidebar has a tree view with 'Policy & Objects' selected, expanded to show 'Policy' (with 'IPv4', 'DoS', 'Proxy Options', 'SSL/SSH Inspection') and 'Objects' (with 'Addresses' selected). The main pane shows a table titled 'Address (1)' with one entry: 'PrivateSubnet' (Type: Subnet, Details: 10.0.1.0/24, Interface: Any, Visibility: checked). There are buttons for 'Create New', 'Edit', and 'Delete' at the top of the table.

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

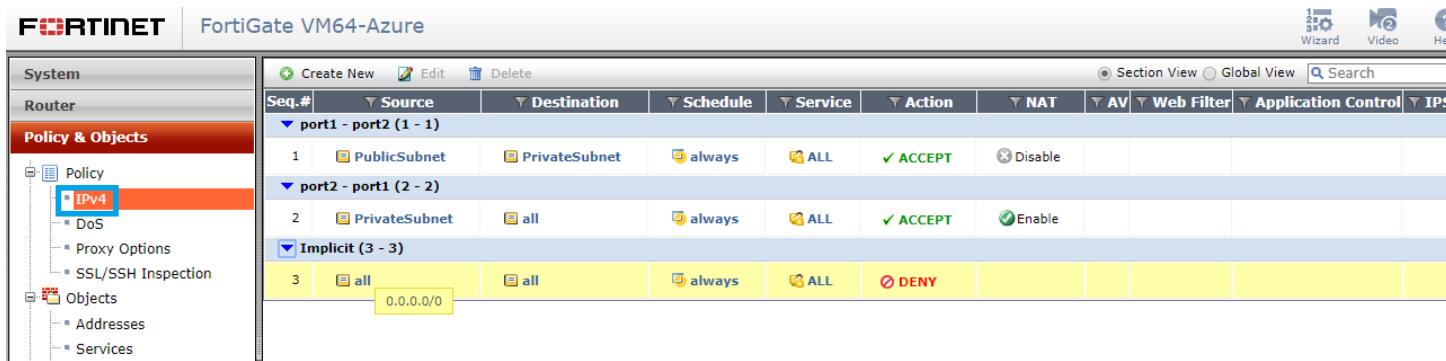
fortigate (3) # set action accept

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.



The screenshot shows the FortiGate VM64-Azure interface under the **Policy & Objects** tab. The left sidebar lists **System**, **Router**, and **Policy & Objects**. Under **Policy & Objects**, **IPv4** is selected, highlighted with a red background. The main pane displays a table of IPv4 policies:

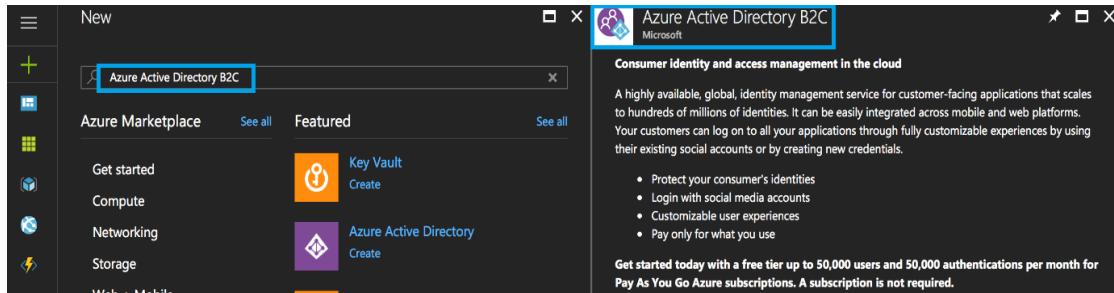
Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS
1	PublicSubnet	PrivateSubnet	always	ALL	✓ ACCEPT	Disable				
2	PrivateSubnet	all	always	ALL	✓ ACCEPT	Enable				
3	all	all	always	ALL	✗ DENY					

4.2. Azure B2C Tenant Creation and Configuration

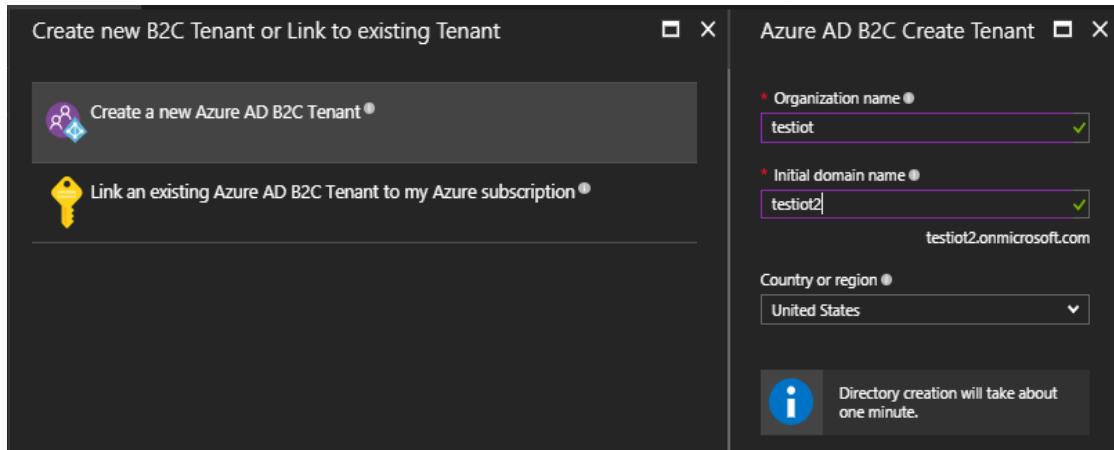
Creating Azure AD B2C tenant is a one-time activity, if you have a B2C Tenant already created by your admin then you should be added into that tenant as Global Administrator to register your app to get the B2C tenant id, application id and sign-in/sign-up policies.

Follow Below steps to create Azure AD B2C Tenant:

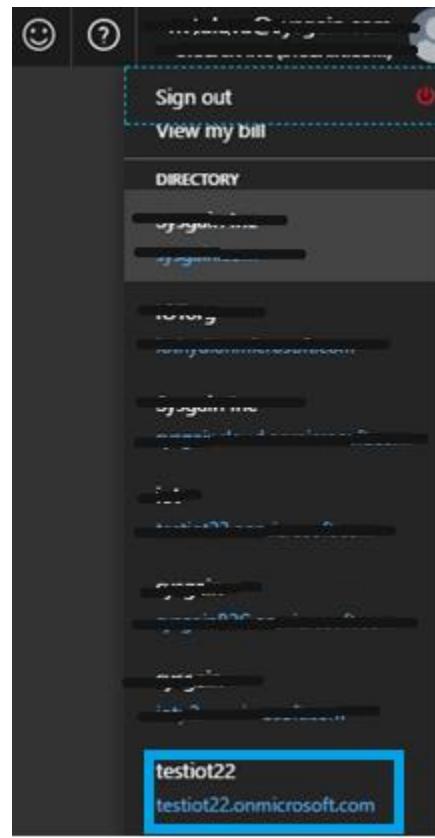
1. Create a new B2C tenant in **Azure Active Directory B2C**. You'll be shown a page with the information on Azure Active Directory B2C. Click **Create** at the bottom to start configuring your new Azure Active Directory B2C tenant.



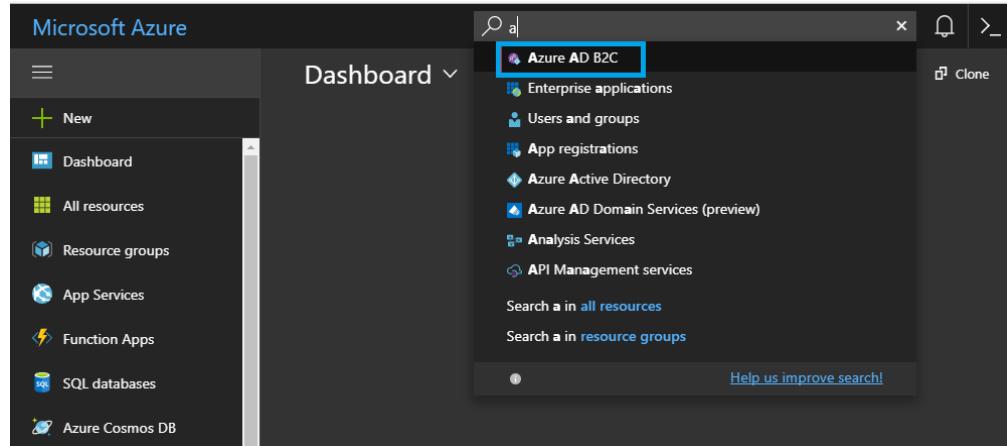
2. Choose the **Organization name**, **Initial Domain name** and **Country or Region** for your Tenant.



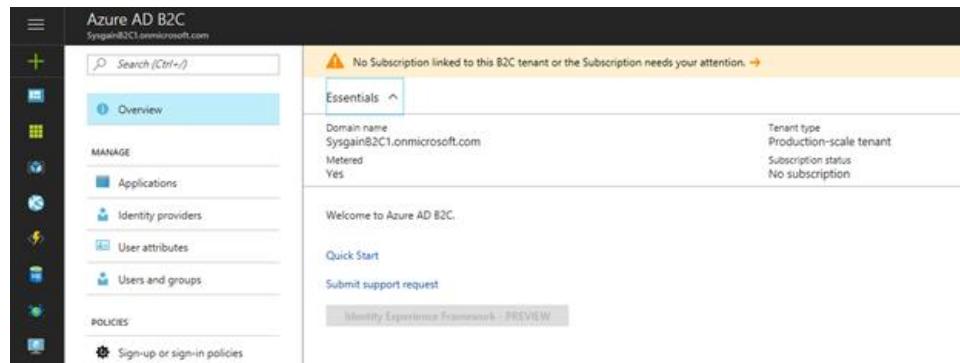
3. Once the B2C Tenant is created, you will see the below confirmation under the portal login user name.



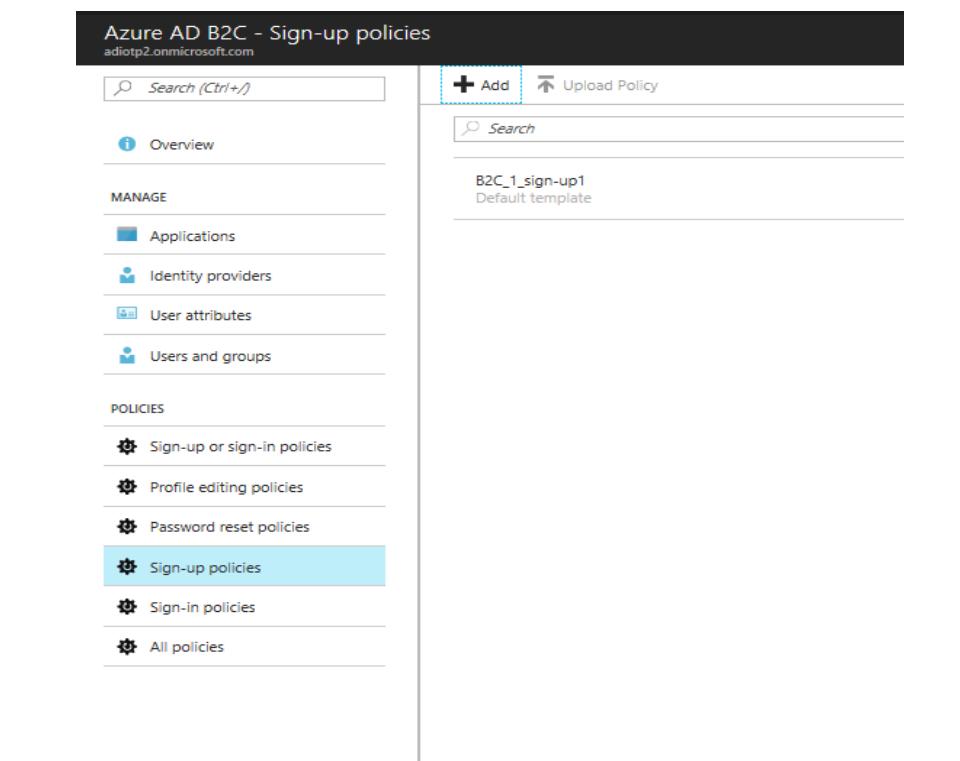
4. Switch to your created tenant by clicking on Created tenant under signout. Type Azure in search column select and click on Azure AD B2C.



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



The screenshot shows the Azure AD B2C Overview page for the tenant SysgainB2C.onmicrosoft.com. A yellow warning bar at the top states: "No Subscription linked to this B2C tenant or the Subscription needs your attention." Below this, the "Essentials" section displays the domain name (SysgainB2C.onmicrosoft.com), metered status (Yes), tenant type (Production-scale tenant), and subscription status (No subscription). The main content area includes a "Welcome to Azure AD B2C" message, a "Quick Start" button, and a "Submit support request" link. A "Identity Experience Framework - PREVIEW" button is also present.



The screenshot shows the Azure AD B2C Sign-up policies page for the tenant adiotp2.onmicrosoft.com. The left sidebar lists various policy categories, with "Sign-up or sign-in policies" currently selected. On the right, there is a search bar and a list of existing policies, including "B2C_1_sign-up1" (Default template).

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

Add policy X

New sign-up policy

* Name i
sign-up1 ✓

* Identity providers i
1 Selected >

Sign-up attributes i
0 Selected >

Application claims i
0 Selected >

Multifactor authentication i
Off >

Page UI customization i
Default >

Create OK

Select identity providers

<input checked="" type="checkbox"/> NAME	IDENTITY PROVIDER
<input checked="" type="checkbox"/> Email signup	Local Account

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

Add policy X

New sign-up policy

* Name i
sign-up1 ✓

* Identity providers i
1 Selected >

Sign-up attributes i
0 Selected >

Application claims i
0 Selected >

Multifactor authentication i
Off >

Page UI customization i
Default >

Create OK

Select sign-up attributes

<input checked="" type="checkbox"/> NAME	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
<input checked="" type="checkbox"/> City	String	The city in which the user is located.	Built-in
<input checked="" type="checkbox"/> Country/Region	String	The country/region in which the user is located.	Built-in
<input checked="" type="checkbox"/> Display Name	String	Display Name of the User	Built-in
<input checked="" type="checkbox"/> Email Address	String		Built-in
<input checked="" type="checkbox"/> Given Name	String	The user's given name (also known as first name).	Built-in
<input checked="" type="checkbox"/> Job Title	String	The user's job title.	Built-in
<input checked="" type="checkbox"/> Postal Code	String	The postal code of the user's address.	Built-in
<input checked="" type="checkbox"/> State/Province	String	The state or province in user's address.	Built-in
<input checked="" type="checkbox"/> Street Address	String	The street address where the user is located	Built-in
<input checked="" type="checkbox"/> Surname	String	The user's surname (also known as family name or last name).	Built-in

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 >

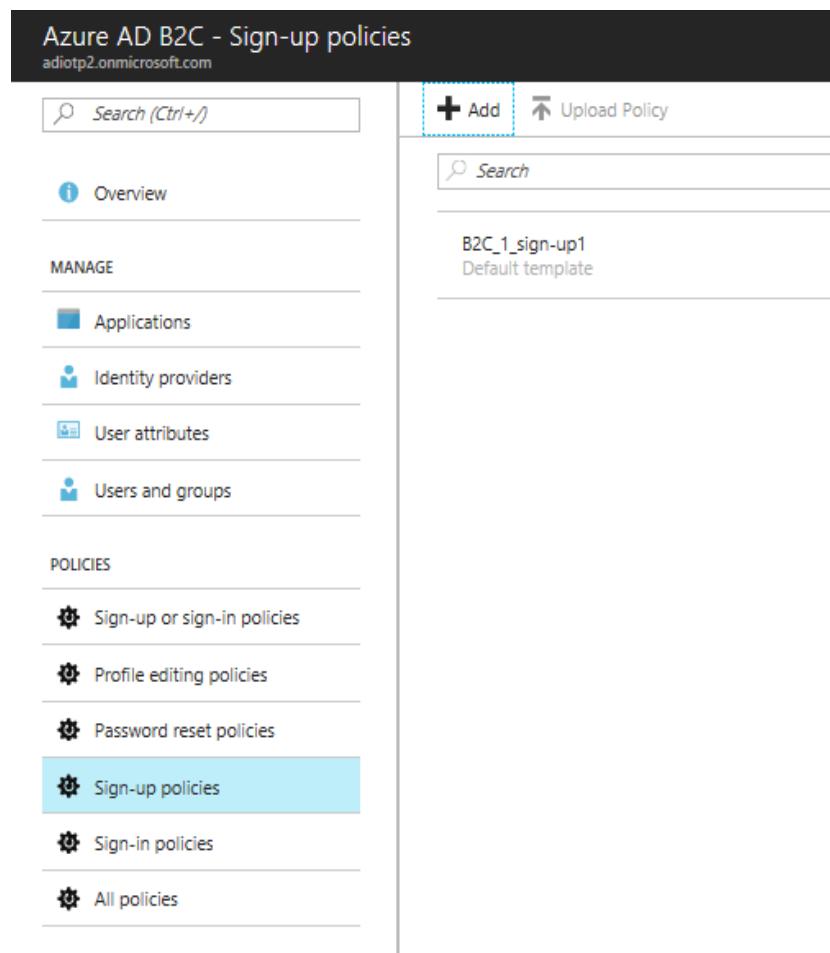
Application claims ⓘ
13 Selected >

Multifactor authentication ⓘ
Off >

Page UI customization ⓘ
Default >

Create

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



The screenshot shows the Azure AD B2C - Sign-up policies interface. The left sidebar has a search bar at the top, followed by sections for Overview, MANAGE (Applications, Identity providers, User attributes, Users and groups), and POLICIES (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Sign-up policies' section is highlighted with a blue background. The main area shows a policy named 'B2C_1_sign-up1' with the status 'Default template'. At the top right, there are 'Add' and 'Upload Policy' buttons, and a search bar.

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

Azure AD B2C - Sign-in policies
adiotp2.onmicrosoft.com

Search (Ctrl+ /)

Overview

MANAGE

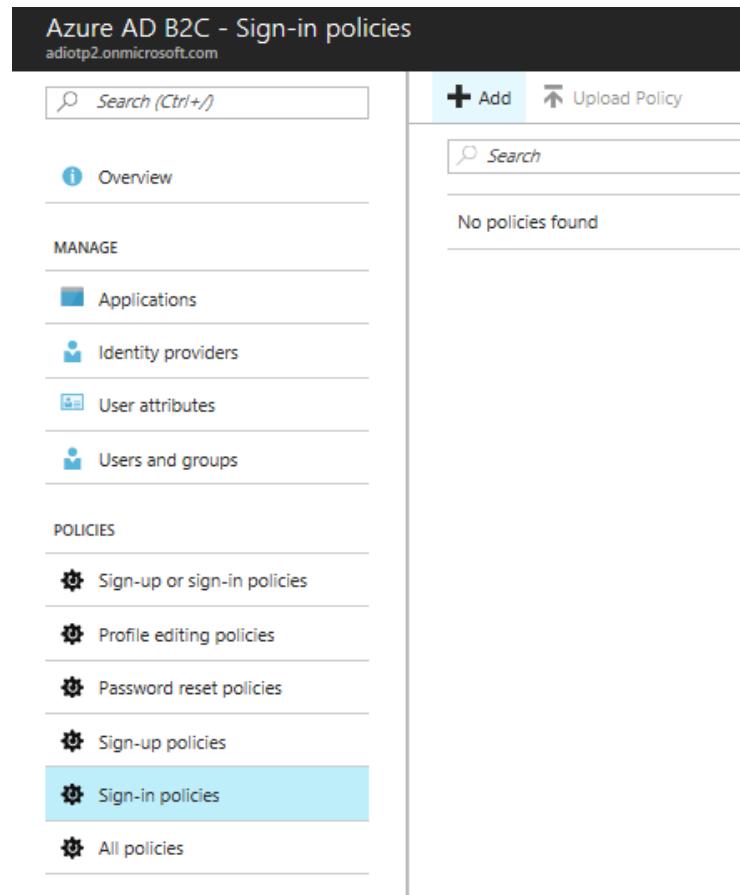
- Applications
- Identity providers
- User attributes
- Users and groups

POLICIES

- Sign-up or sign-in policies
- Profile editing policies
- Password reset policies
- Sign-up policies
- Sign-in policies**
- All policies

+ Add Upload Policy

No policies found



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

Add policy

New sign-in policy

NAME	IDENTITY PROVIDER
<input checked="" type="checkbox"/> Local Account Signin	Local Account Signin

Name: sign-in1

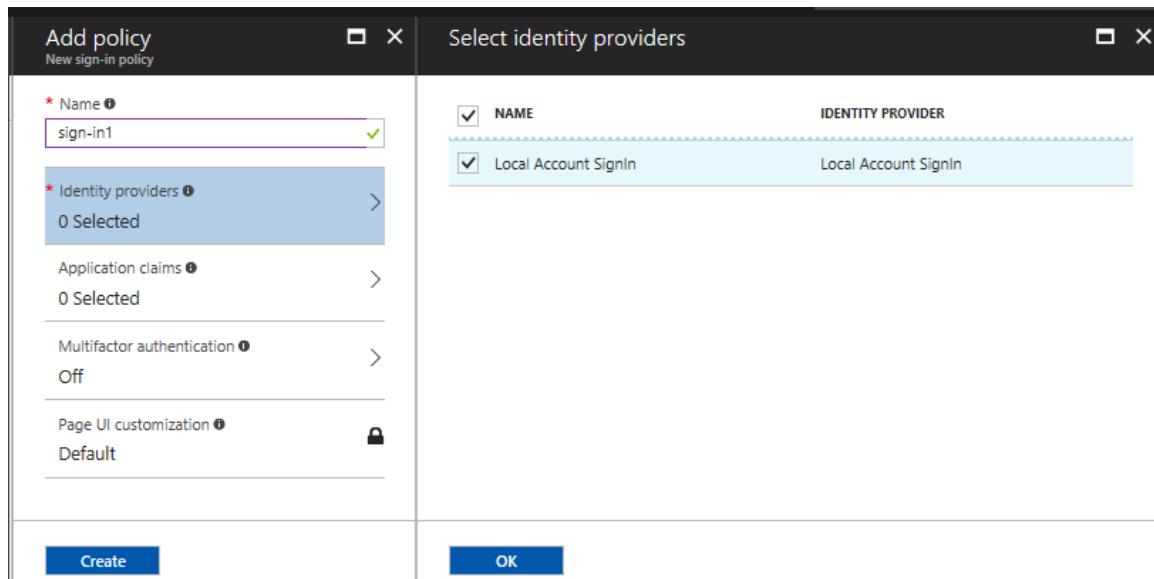
Identity providers: 0 Selected

Application claims: 0 Selected

Multifactor authentication: Off

Page UI customization: Default

Create **OK**



11. Select all Application claim

Add policy
New sign-in policy

- * Name
- * Identity providers
- Application claims >
- Multifactor authentication
- Page UI customization

Select application claims

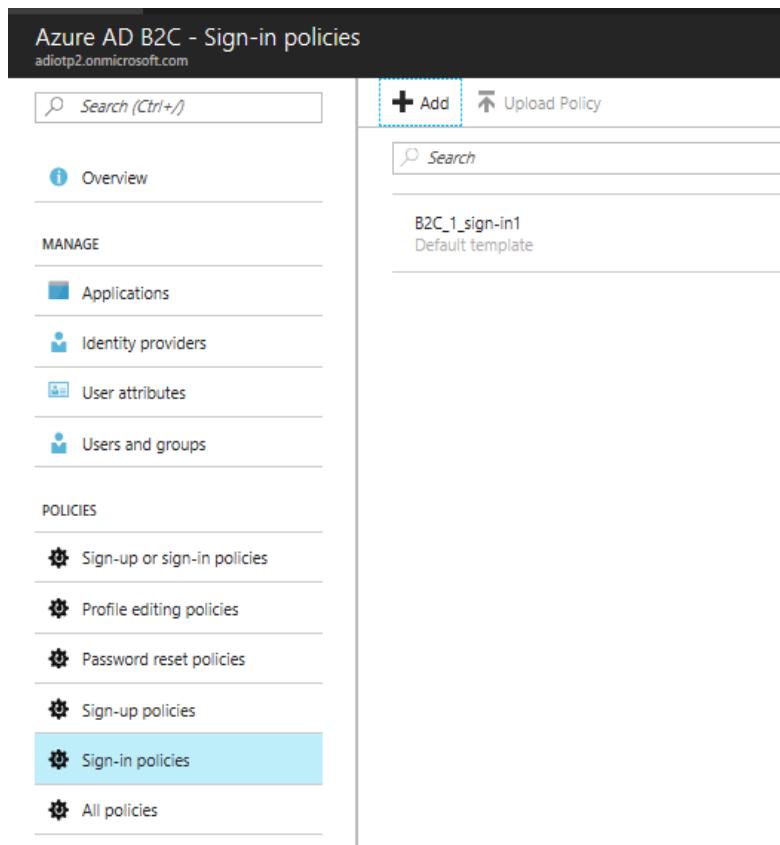
<input checked="" type="checkbox"/>	NAME	CLAIM TYPE	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
<input checked="" type="checkbox"/>	City	city	String	The city in which the user is located.	Built-in
<input checked="" type="checkbox"/>	Country/Region	country	String	The country/region in which the user is located.	Built-in
<input checked="" type="checkbox"/>	Display Name	displayName	String	Display Name of the User	Built-in
<input checked="" type="checkbox"/>	Email Addresses	emails	StringCollection	Email addresses of the user.	Built-in
<input checked="" type="checkbox"/>	Given Name	givenName	String	The user's given name (also known as first name).	Built-in
<input checked="" type="checkbox"/>	Identity Provider	identityProvider	String	The social identity provider used by the user to access to your ap...	Built-in
<input checked="" type="checkbox"/>	Job Title	jobTitle	String	The user's job title.	Built-in
<input checked="" type="checkbox"/>	Postal Code	postalCode	String	The postal code of the user's address.	Built-in
<input checked="" type="checkbox"/>	State/Province	state	String	The state or province in user's address.	Built-in
<input checked="" type="checkbox"/>	Street Address	streetAddress	String	The street address where the user is located	Built-in
<input checked="" type="checkbox"/>	Surname	surname	String	The user's surname (also known as family name or last name).	Built-in
<input checked="" type="checkbox"/>	User's Object ID	objectId	String	Object identifier (ID) of the user object in Azure AD.	Built-in

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

Add policy
New sign-in policy

- * Name
- * Identity providers
- Application claims >
- Multifactor authentication
- Page UI customization

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



The screenshot shows the Azure AD B2C - Sign-in policies interface. The left sidebar has sections for Overview, MANAGE (Applications, Identity providers, User attributes, Users and groups), and POLICIES (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Sign-in policies' link is highlighted with a blue background. The main area shows a search bar, a '+ Add' button, and an 'Upload Policy' button. Below is a list of policies: 'B2C_1_sign-in1' (Default template).

14. Click on **Profile editing policies**

Azure AD B2C - Profile editing policies
adidtp2.onmicrosoft.com

Search (Ctrl+ /)

Overview

MANAGE

- Applications
- Identity providers
- User attributes
- Users and groups

POLICIES

- Sign-up or sign-in policies
- Profile editing policies

Profile editing policies is highlighted.

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

Add policy

New profile editing policy

* Name profile-edit1

* Identity providers 0 Selected

Profile attributes 0 Selected

Application claims 0 Selected

Page UI customization Default

Create

Select identity providers

NAME	IDENTITY PROVIDER
<input checked="" type="checkbox"/> Local Account SignIn	Local Account SignIn

OK

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

Add policy

New profile editing policy

* Name profile-edit1

* Identity providers 1 Selected

Profile attributes 0 Selected

Application claims 0 Selected

Page UI customization Default

Select profile attributes

NAME	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	String	The city in which the user is located.	Built-in
Country/Region	String	The country/region in which the user is located.	Built-in
Display Name	String	Display Name of the User	Built-in
Given Name	String	The user's given name (also known as first name).	Built-in
Job Title	String	The user's job title.	Built-in
Postal Code	String	The postal code of the user's address.	Built-in
State/Province	String	The state or province in user's address.	Built-in
Street Address	String	The street address where the user is located	Built-in
Surname	String	The user's surname (also known as family name or last name).	Built-in

Create OK

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

Add policy

New profile editing policy

* Name profile-edit1

* Identity providers 1 Selected

Profile attributes 9 Selected

Application claims 0 Selected

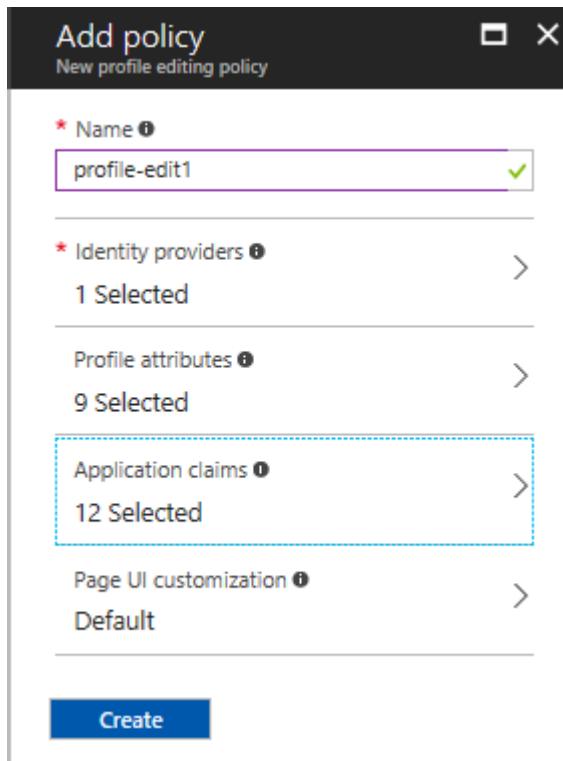
Page UI customization Default

Select application claims

NAME	CLAIM TYPE	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	city	String	The city in which the user is located.	Built-in
Country/Region	country	String	The country/region in which the user is located.	Built-in
Display Name	displayName	String	Display Name of the User	Built-in
Email Addresses	emails	StringCollection	Email addresses of the user.	Built-in
Given Name	givenName	String	The user's given name (also known as first name).	Built-in
Identity Provider	identityProvider	String	The social identity provider used by the user to access to your ap...	Built-in
Job Title	jobTitle	String	The user's job title.	Built-in
Postal Code	postalCode	String	The postal code of the user's address.	Built-in
State/Province	state	String	The state or province in user's address.	Built-in
Street Address	streetAddress	String	The street address where the user is located	Built-in
Surname	surname	String	The user's surname (also known as family name or last name).	Built-in
User's Object ID	objectId	String	Object identifier (ID) of the user object in Azure AD.	Built-in

Create OK

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

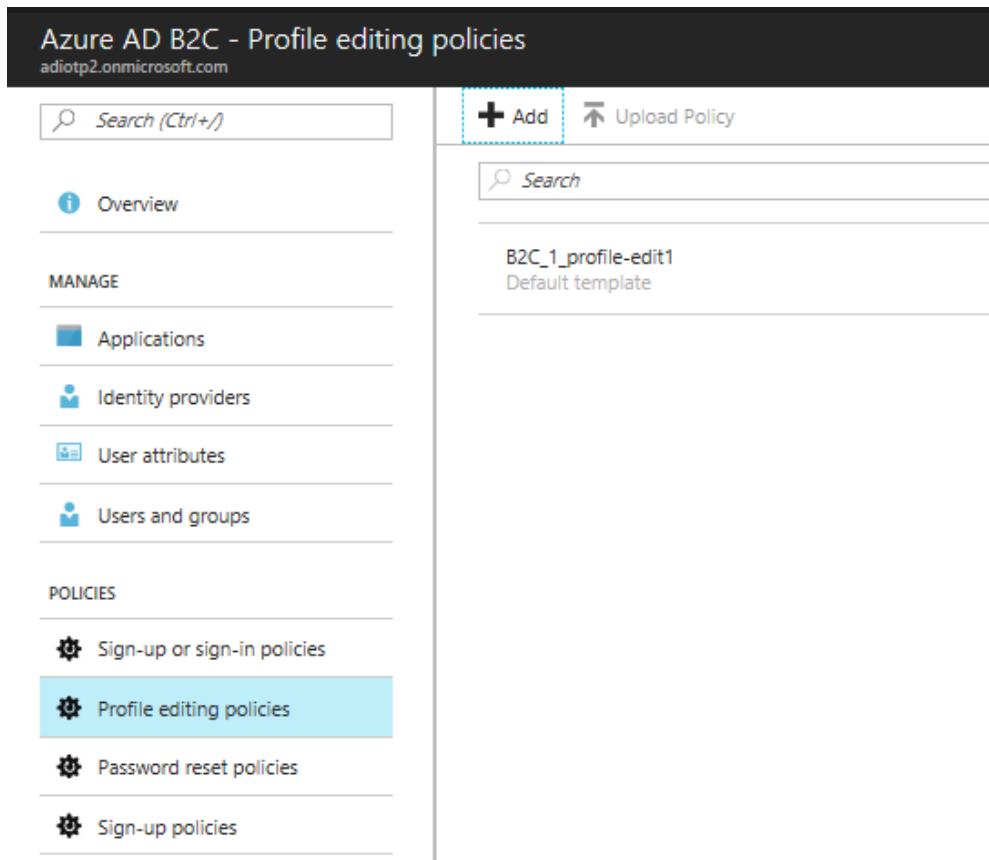


The screenshot shows the 'Add policy' dialog box with the title 'New profile editing policy'. It contains the following fields:

- Name:** profile-edit1 (highlighted with a purple border)
- Identity providers:** 1 Selected
- Profile attributes:** 9 Selected
- Application claims:** 12 Selected (highlighted with a blue dashed border)
- Page UI customization:** Default

A large blue 'Create' button is at the bottom.

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



The screenshot shows the Azure AD B2C - Profile editing policies page. The URL in the address bar is `adiotp2.onmicrosoft.com`. The left sidebar has a search bar at the top with the placeholder `Search (Ctrl+Shift+F)`. Below it are sections for **MANAGE** (Applications, Identity providers, User attributes, Users and groups) and **POLICIES** (Sign-up or sign-in policies, **Profile editing policies**, Password reset policies, Sign-up policies). The **Profile editing policies** item is highlighted with a blue background. The main content area has a search bar at the top with the placeholder `Search`. It displays a single policy named **B2C_1_profile-edit1** with the subtitle **Default template**.

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

Azure AD B2C - Password reset policies
adotp2.onmicrosoft.com

Search (Ctrl+F)

Add **Upload Policy**

No policies found

- Overview**
- MANAGE**
 - Applications**
 - Identity providers**
 - User attributes**
 - Users and groups**
- POLICIES**
 - Sign-up or sign-in policies**
 - Profile editing policies**
 - Password reset policies** **(selected)**
 - Sign-up policies**
 - Sign-in policies**
 - All policies**

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

Add policy X

New password reset policy

* Name i
password-change1

* Identity providers i >
0 Selected

Application claims i >
0 Selected

Multifactor authentication i >
Off

Page UI customization i lock
Default

Create

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

Add policy

New password reset policy

- * Name *
password-change1
- * Identity providers *
0 Selected
- Application claims *
0 Selected
- Multifactor authentication *
Off
- Page UI customization *
Default

Select identity providers

<input checked="" type="checkbox"/> NAME	IDENTITY PROVIDER
<input checked="" type="checkbox"/> Reset password using email address	Local Account

Create
OK

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

Add policy

New password reset policy

- * Name *
password-change1
- * Identity providers *
1 Selected
- Application claims *
0 Selected
- Multifactor authentication *
Off
- Page UI customization *
Default

Select application claims

<input checked="" type="checkbox"/> NAME	CLAIM TYPE	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
<input checked="" type="checkbox"/> City	city	String	The city in which the user is located.	Built-in
<input checked="" type="checkbox"/> Country/Region	country	String	The country/region in which the user is located.	Built-in
<input checked="" type="checkbox"/> Display Name	displayName	String	Display Name of the User	Built-in
<input checked="" type="checkbox"/> Email Addresses	emails	StringCollection	Email addresses of the user.	Built-in
<input checked="" type="checkbox"/> Given Name	givenName	String	The user's given name (also known as first name).	Built-in
<input checked="" type="checkbox"/> Job Title	jobTitle	String	The user's job title.	Built-in
<input checked="" type="checkbox"/> Postal Code	postalCode	String	The postal code of the user's address.	Built-in
<input checked="" type="checkbox"/> State/Province	state	String	The state or province in user's address.	Built-in
<input checked="" type="checkbox"/> Street Address	streetAddress	String	The street address where the user is located	Built-in
<input checked="" type="checkbox"/> Surname	surname	String	The user's surname (also known as family name or last name).	Built-in
<input checked="" type="checkbox"/> User's Object ID	objectId	String	Object identifier (ID) of the user object in Azure AD.	Built-in

Create
OK

24. Click on **Create**.

Add policy □ X

New password reset policy

* Name i
password-change1 ✓

* Identity providers i >
1 Selected

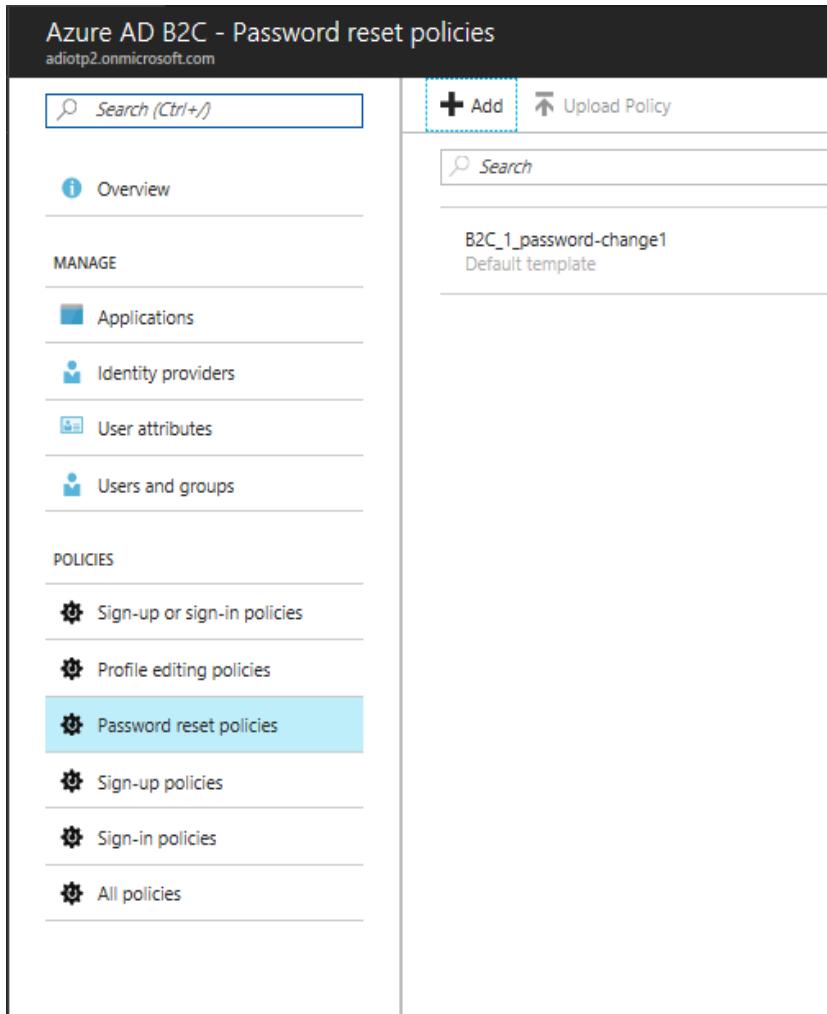
Application claims i >
11 Selected

Multifactor authentication i >
Off

Page UI customization i >
Default

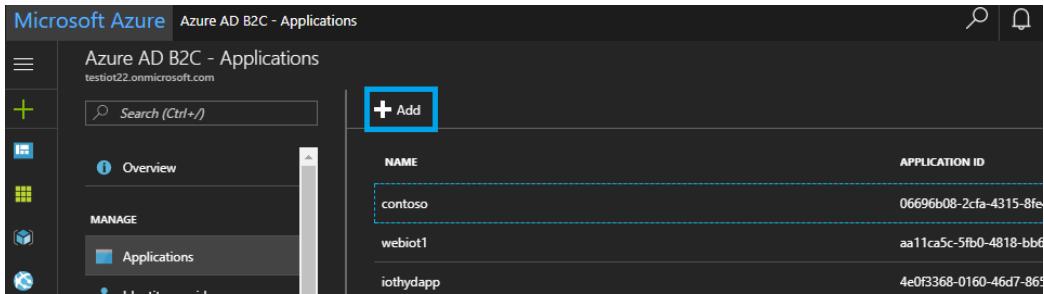
Create

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



The screenshot shows the 'Azure AD B2C - Password reset policies' page. The URL is 'adiotp2.onmicrosoft.com'. The left sidebar has sections for 'Overview', 'MANAGE' (Applications, Identity providers, User attributes, Users and groups), and 'POLICIES' (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Password reset policies' section is highlighted with a blue background. The main area shows a policy named 'B2C_1_password-change1' with the status 'Default template'. There are 'Search' and 'Upload Policy' buttons at the top, and a '+ Add' button on the right.

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



The screenshot shows the 'Microsoft Azure - Azure AD B2C - Applications' page. The URL is 'testiot22.onmicrosoft.com'. The left sidebar has sections for 'Overview', 'MANAGE' (Applications, Identity providers, User attributes, Groups, Devices), and 'POLICIES' (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Applications' section is highlighted with a blue background. The main area shows three applications: 'contoso', 'webiot1', and 'iothydapp'. The 'contoso' application is selected, showing its details. There is a '+ Add' button on the right. A search bar and a refresh icon are at the top right.

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:

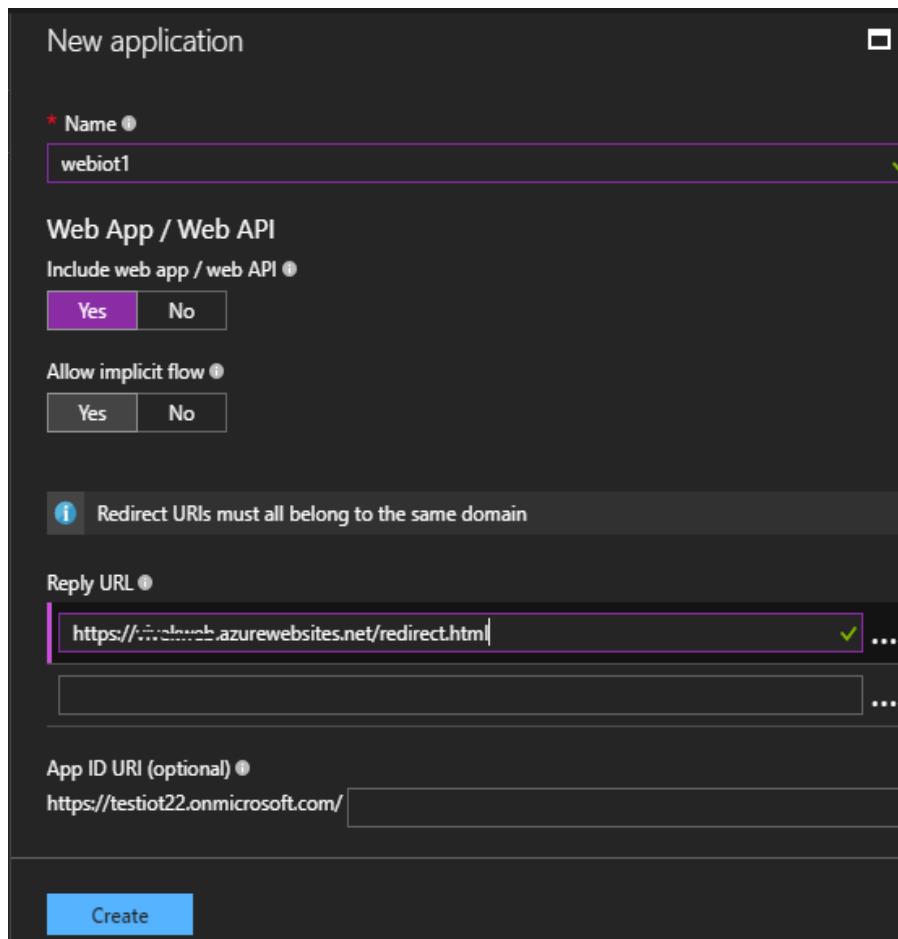
`https://<name of the web app>.azurewebsites.net/redirect.html`

During the web app registration with PowerBI, we will use this reply URL.

Example: <https://iotweb.azurewebsites.net/redirect.html>

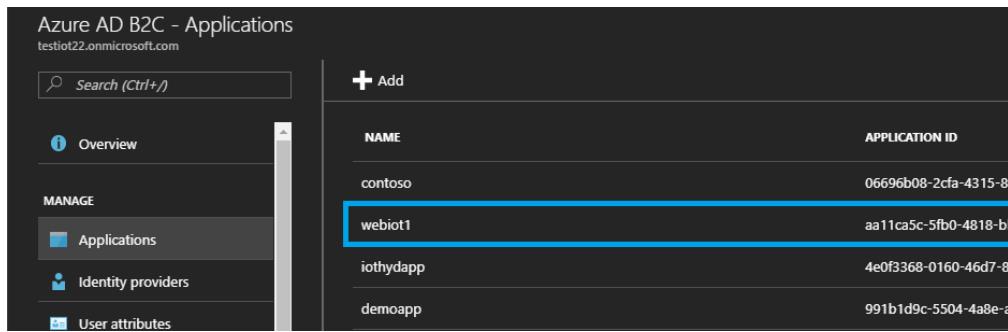
After that, click on **Create**.

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



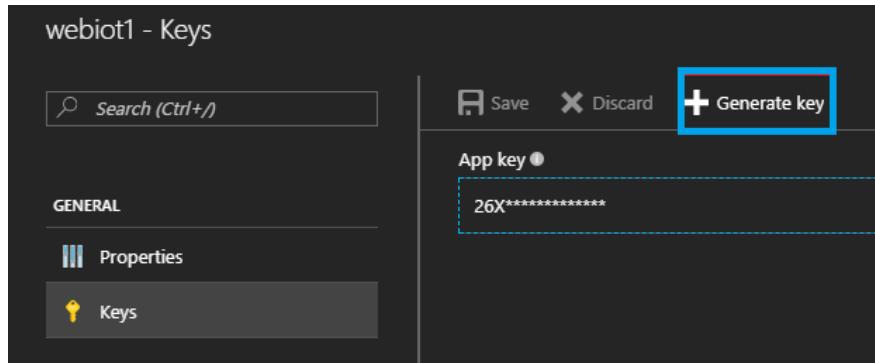
The screenshot shows the 'New application' dialog in the Azure AD B2C interface. The application name is 'webiot1'. The 'Web App / Web API' tab is selected, with 'Include web app / web API' set to 'Yes'. The 'Allow implicit flow' setting is 'No'. A note indicates that 'Redirect URIs must all belong to the same domain'. The 'Reply URL' field contains 'https://testiot22.azurewebsites.net/redirect.html'. An optional 'App ID URI' is listed as 'https://testiot22.onmicrosoft.com/'. A 'Create' button is at the bottom.

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

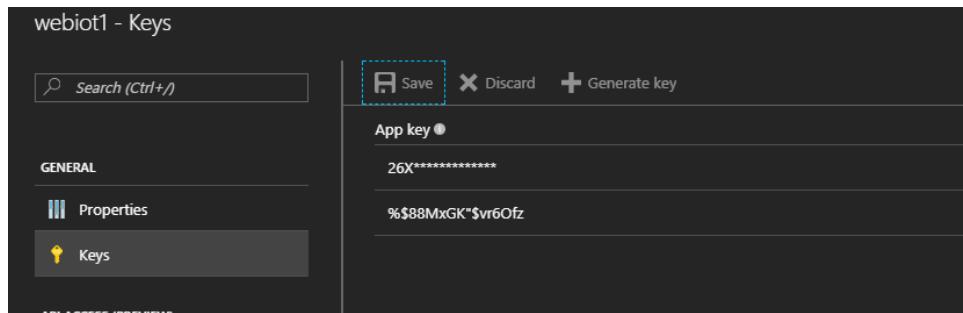


NAME	APPLICATION ID
contoso	06696b08-2cfa-4315-8e0d-000000000000
webiot1	aa11ca5c-5fb0-4818-bb0f-000000000000
iothydapp	4e0f3368-0160-46d7-8e0d-000000000000
demoapp	991b1d9c-5504-4a8e-a20d-000000000000

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



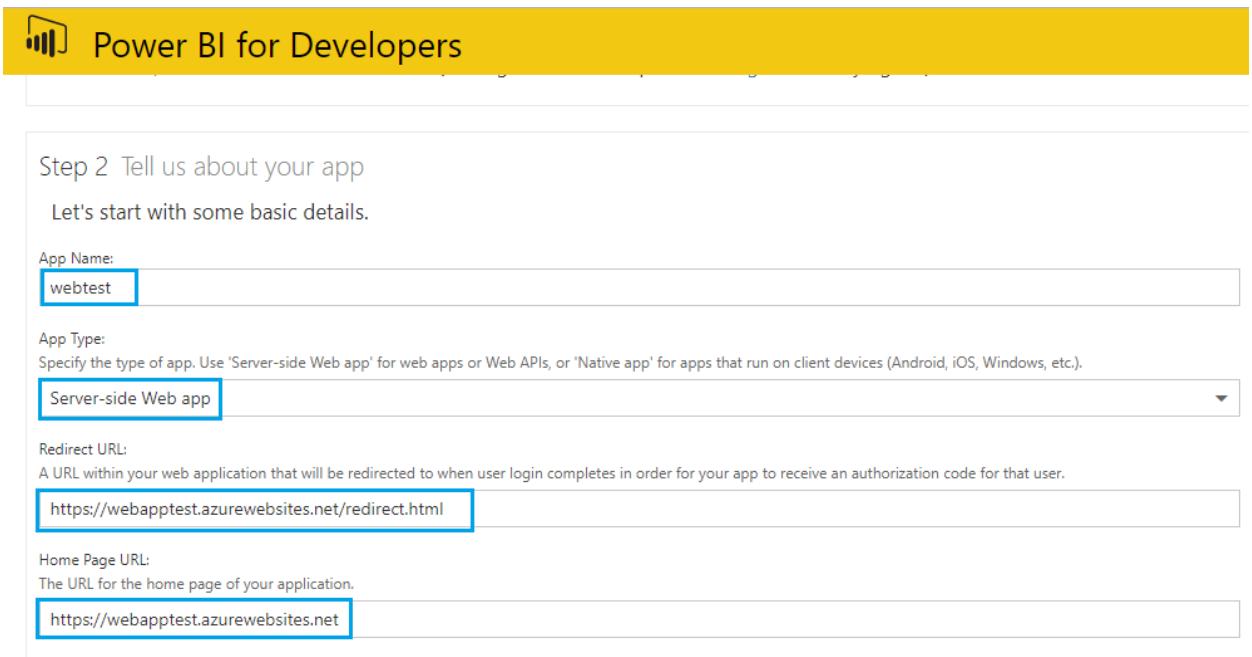
30. **Copy** the secret key.



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.



The screenshot shows the 'Step 2 Tell us about your app' section of the Power BI for Developers registration process. It includes fields for App Name, App Type, Redirect URL, and Home Page URL, each with its respective value highlighted by a blue border.

Step 2 Tell us about your app

Let's start with some basic details.

App Name:
webtest

App Type:
Specify the type of app. Use 'Server-side Web app' for web apps or Web APIs, or 'Native app' for apps that run on client devices (Android, iOS, Windows, etc.).
Server-side Web app

Redirect URL:
A URL within your web application that will be redirected to when user login completes in order for your app to receive an authorization code for that user.
<https://webapptest.azurewebsites.net/redirect.html>

Home Page URL:
The URL for the home page of your application.
<https://webapptest.azurewebsites.net>

- 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.

Step 3 Choose APIs to access

Select the APIs and the level of access your app needs.

Dataset APIs

- Read All Datasets
- Read and Write All Datasets

Report and Dashboard APIs

- Read All Dashboards
- Read All Reports
- Read and Write All Reports

Other APIs

- Read All Groups
- Create Content

Step 4 Register your app

Once you've set everything the way you want it, click the button below and we'll register your app. Your client ID and secret (for web apps only) will appear below. Be sure to copy the values into your app. By clicking the Register App button, you have accepted the [terms of use](#).

[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.



Power BI for Developers

Step 4 Register your app

Once you've set everything the way you want it, click the button below and we'll register your app. Your client ID and secret (for web apps only) will appear below. Be sure to copy the values into your app. By clicking the Register App button, you have accepted the [terms of use](#).

[Register App](#)

Client ID:

c33aad30-5e30-426f-8140-1b4a0c63b9b3

Client Secret:

oA6639cMkKuDrvZQZsQ6/BMd8imml2xDkrbnvoqw+c==

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.

Microsoft Azure | sysgain inc - App registrations

sysgain inc - App registrations
Azure Active Directory

+ New application registration Endpoints Troubleshoot

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).

webtest | All apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
WE webtest	Web app / API	b9f01ad1-fc99-49c6-a136-06ae..

OVERVIEW

Quick start

MANAGE

- Users and groups
- Enterprise applications
- App registrations**
- Application proxy
- Licenses
- Azure AD Connect
- Domain names
- Mobility (MDM and MAM)

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

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

Settings

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

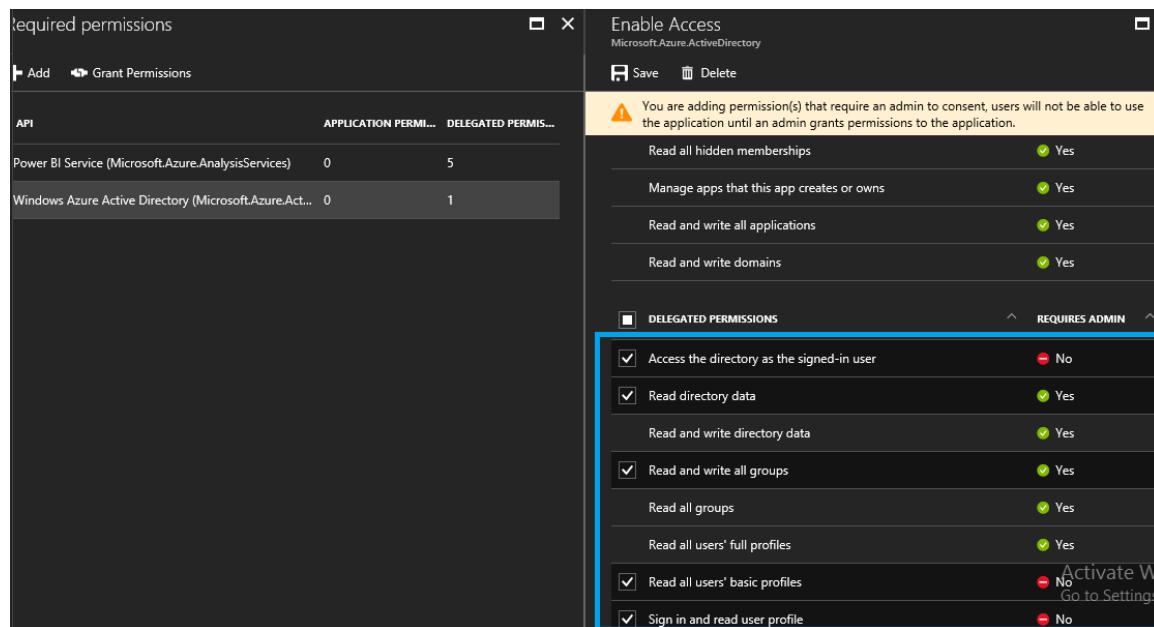
Required permissions

+ Add Grant Permissions

API	APPLICATION PERMI...	DELEGATED PERMI...
Power BI Service (Microsoft.Azure.AnalysisServices)	0	5
Windows Azure Active Directory (Microsoft.Azure.Act...	0	1

- 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**.



The screenshot shows two side-by-side Azure portal pages.

Required permissions:

- Add API: Microsoft.Azure.AnalysisServices
- Grant Permissions
- API: Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)
- APPLICATION PERMISSIONS: 0
- DELEGATED PERMISSIONS: 5

Enable Access: Microsoft.Azure.ActiveDirectory

You are adding permission(s) that require an admin to consent; users will not be able to use the application until an admin grants permissions to the application.

Permission	Requires Admin
Read all hidden memberships	Yes
Manage apps that this app creates or owns	Yes
Read and write all applications	Yes
Read and write domains	Yes
DELEGATED PERMISSIONS	
Access the directory as the signed-in user	No
<input checked="" type="checkbox"/> Read directory data	Yes
Read and write directory data	Yes
<input checked="" type="checkbox"/> Read and write all groups	Yes
Read all groups	Yes
Read all users' full profiles	Yes
<input checked="" type="checkbox"/> Read all users' basic profiles	No
<input checked="" type="checkbox"/> Sign in and read user profile	No

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

Required permissions

+ Add 

API	APPLICATION PERMIS...	DELEGATED PERMIS...
Power BI Service (Microsoft.Azure.AnalysisServices)	0	5
Windows Azure Active Directory (Microsoft.Azure.Act...	0	5

Enable Access

 Save 

You are adding permission(s) to your application, users will have to consent even if they've already done so previously.

No application permissions available.

 DELEGATED PERMISSIONS 

	REQUIRES ADMIN
Add data to a user's dataset (preview)	<input type="radio"/> No
<input checked="" type="checkbox"/> View all Dashboards (preview)	<input type="radio"/> No
<input checked="" type="checkbox"/> View all Datasets	<input type="radio"/> No
<input checked="" type="checkbox"/> Read and Write all Datasets	<input type="radio"/> No
<input checked="" type="checkbox"/> View content properties (preview)	<input type="radio"/> No
<input checked="" type="checkbox"/> Create content (preview)	<input type="radio"/> No
<input checked="" type="checkbox"/> View all Reports (preview)	<input type="radio"/> No
View all Groups	<input type="radio"/> No
<input checked="" type="checkbox"/> View users Groups	<input type="radio"/> No
<input checked="" type="checkbox"/> Read and Write all Reports	<input type="radio"/> No

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

Settings

Filter settings

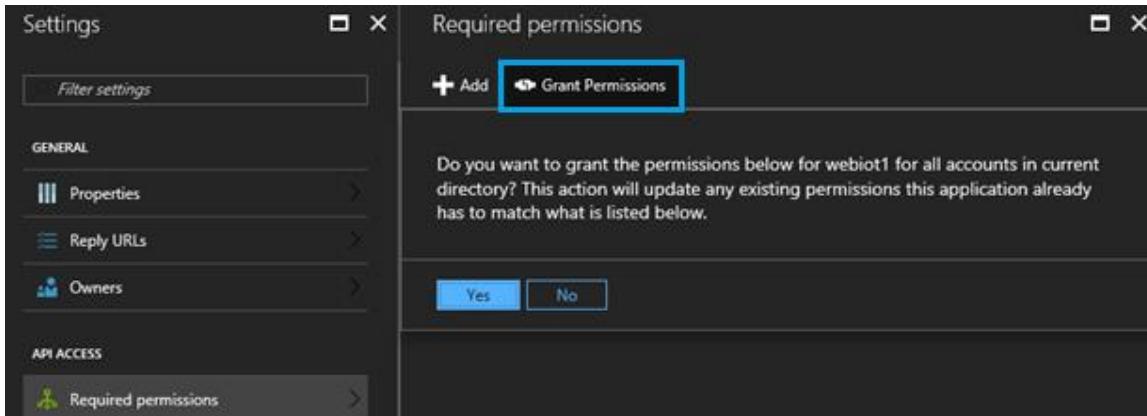
- GENERAL
 - Properties
 - Reply URLs
 - Owners
- API ACCESS
 -  Required permissions
 - Keys
- TROUBLESHOOTING + SUPPORT
 - Troubleshoot
 - New support request

Required permissions

+ Add 

API	APPLICATION PERMIS...	DELEGATED PERMIS...
Power BI Service (Microsoft.Azure.AnalysisServices)	0	8
Windows Azure Active Directory (Microsoft.Azure.Act...	0	5

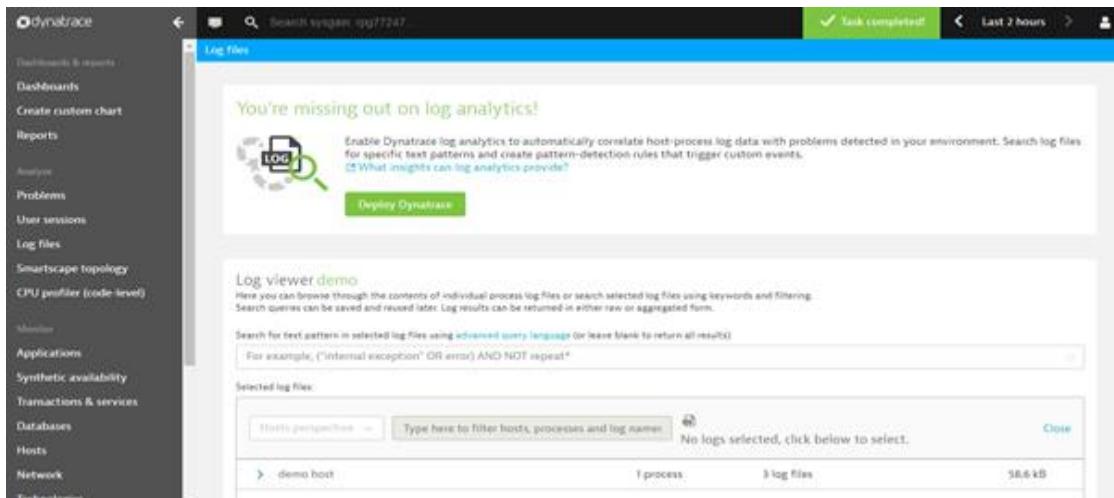
7. Click on **Grant Permissions**, then click **Yes**.



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.

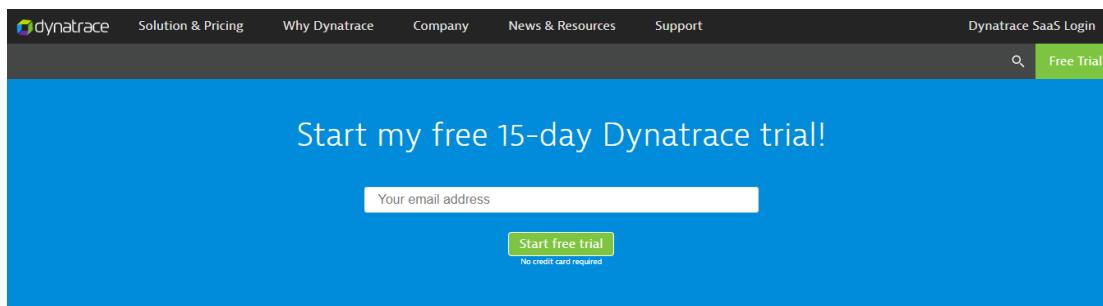
New Users: Please follow the below steps for "Sign up to Dynatrace trial SaaS for 15 days."

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

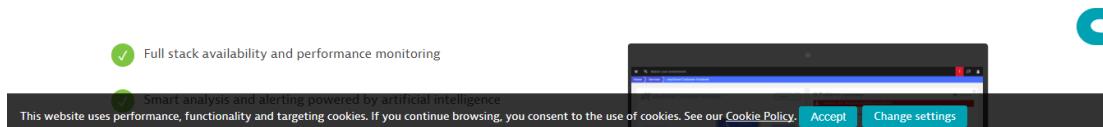
Support URL: <https://www.dynatrace.com/support/>

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

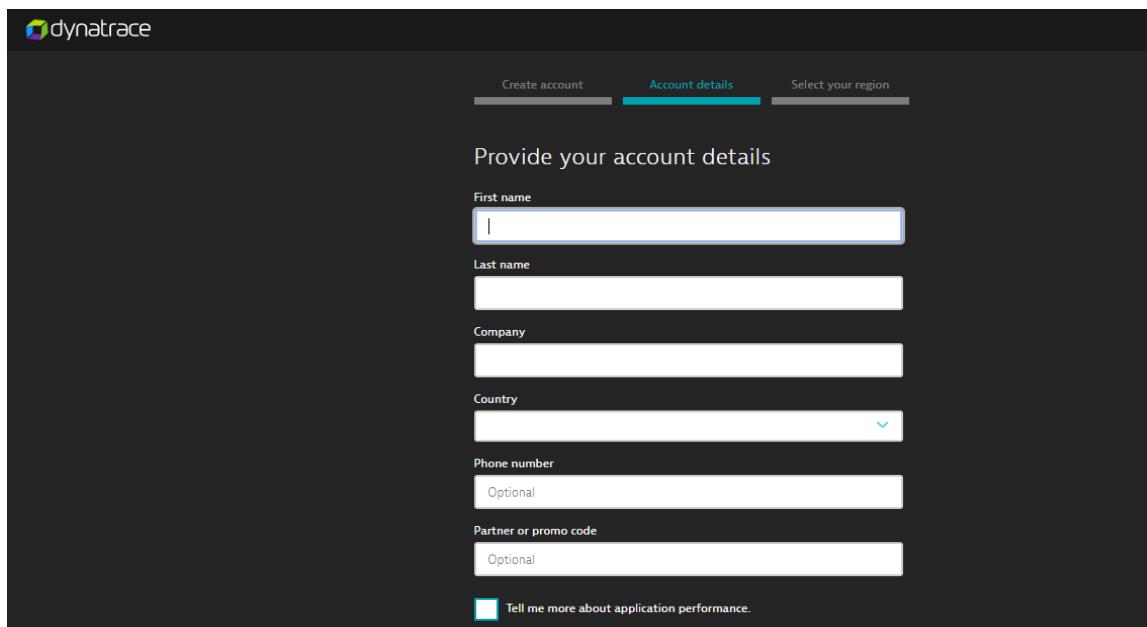
Dynatrace home page - <https://www.dynatrace.com>



Get started now with Dynatrace SaaS or [contact us](#) for Dynatrace on-premises!

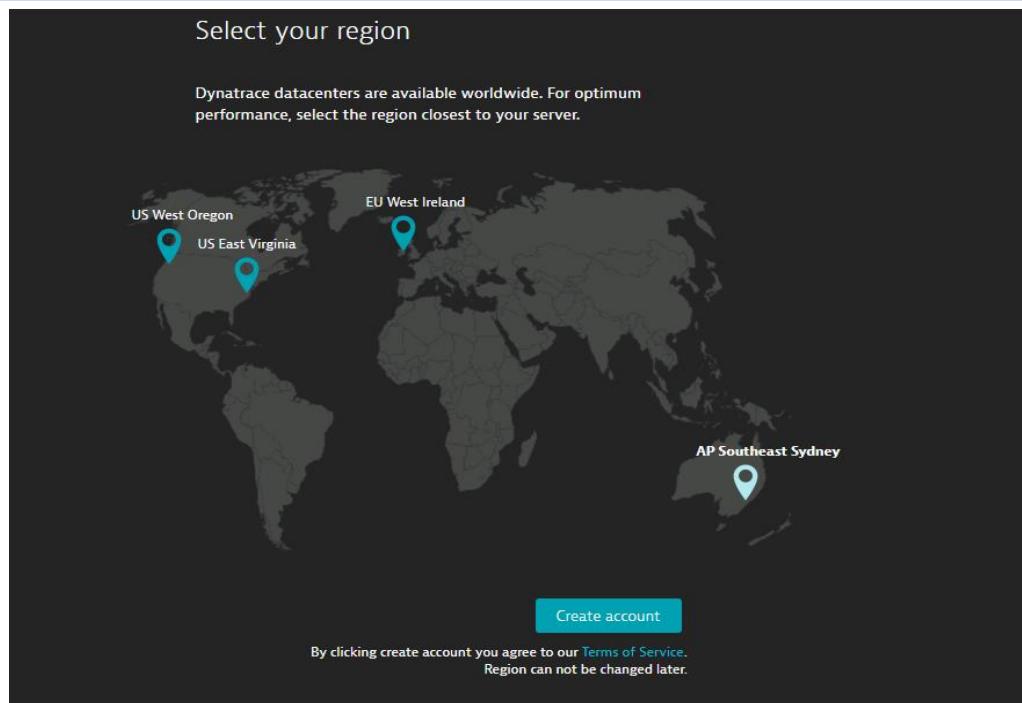


2. The below screen will appear. Fill out the **Create account**, **Account details** and **Select your region** screens.

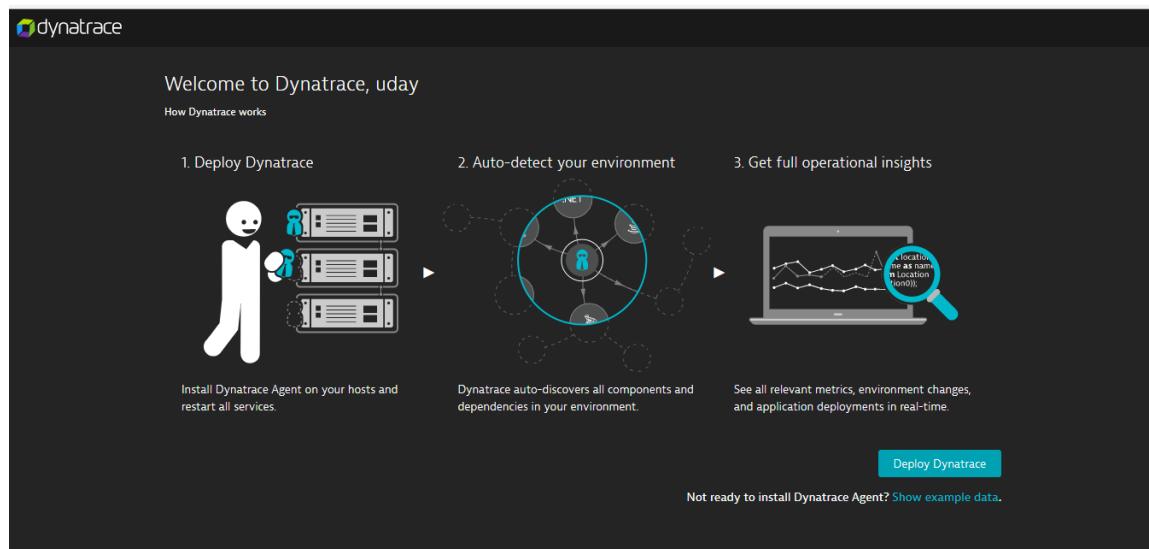


The screenshot shows a "Provide your account details" form. The form is set against a dark background and includes fields for "First name", "Last name", "Company", "Country" (a dropdown menu), "Phone number", and "Partner or promo code". There is also a checkbox for "Tell me more about application performance". Above the form, there are three tabs: "Create account" (disabled), "Account details" (highlighted in blue), and "Select your region".

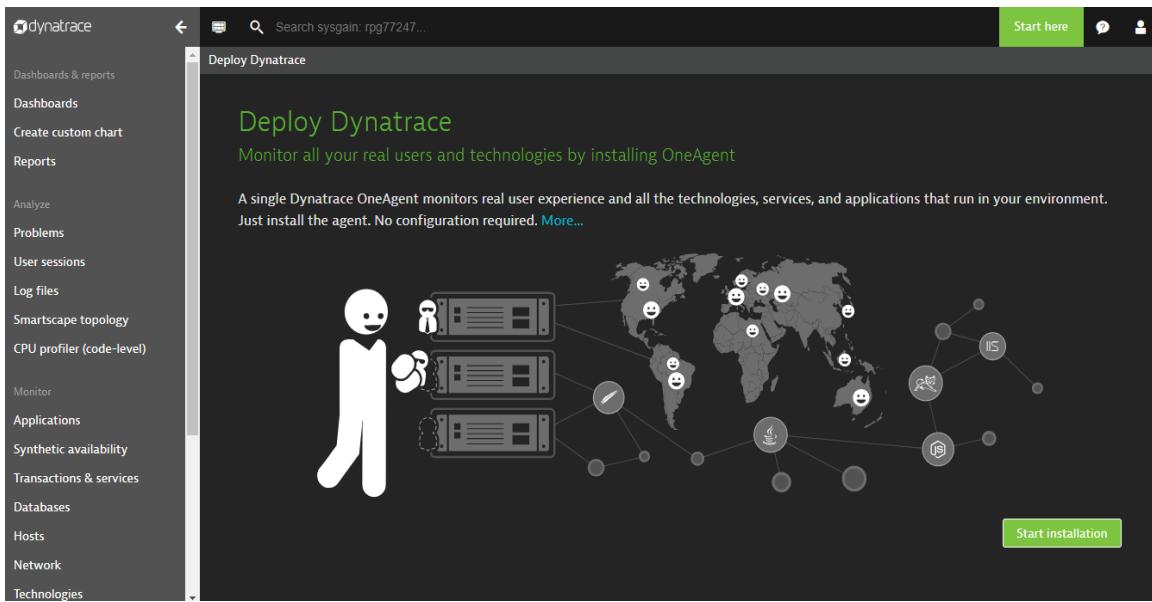
3. Select your region and click on “**Create account**”.



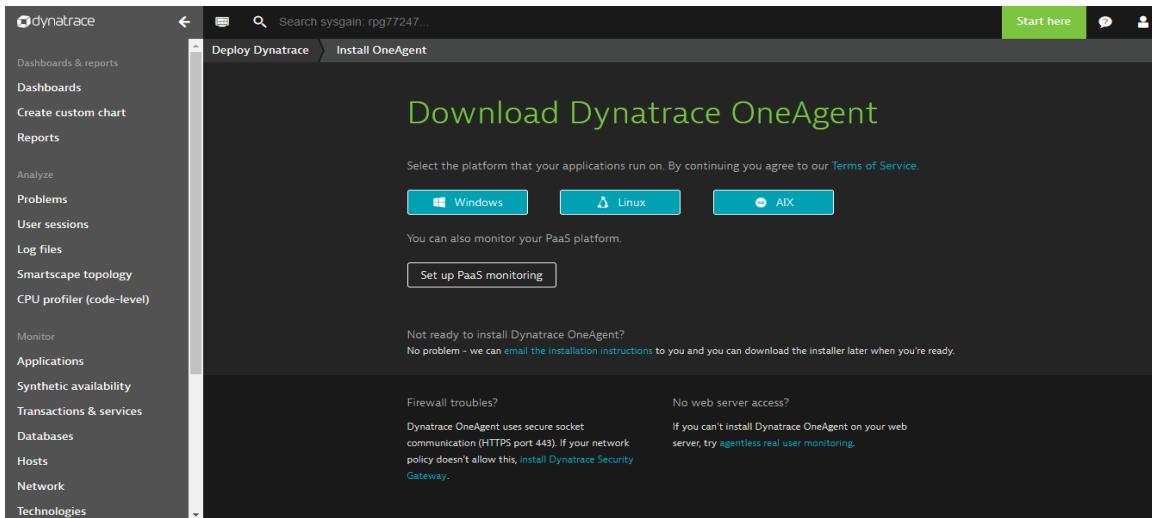
4. Click on “**Deploy Dynatrace**”.



5. Click on “**Start installation**”.



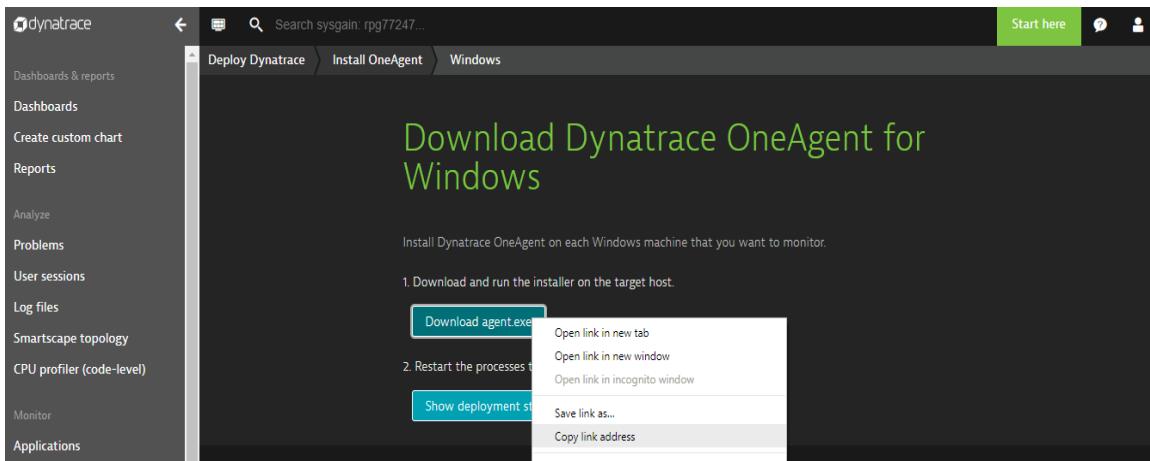
- On the next screen, click "**Windows**".



- 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 redirect 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)	
senderEmailPasword	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

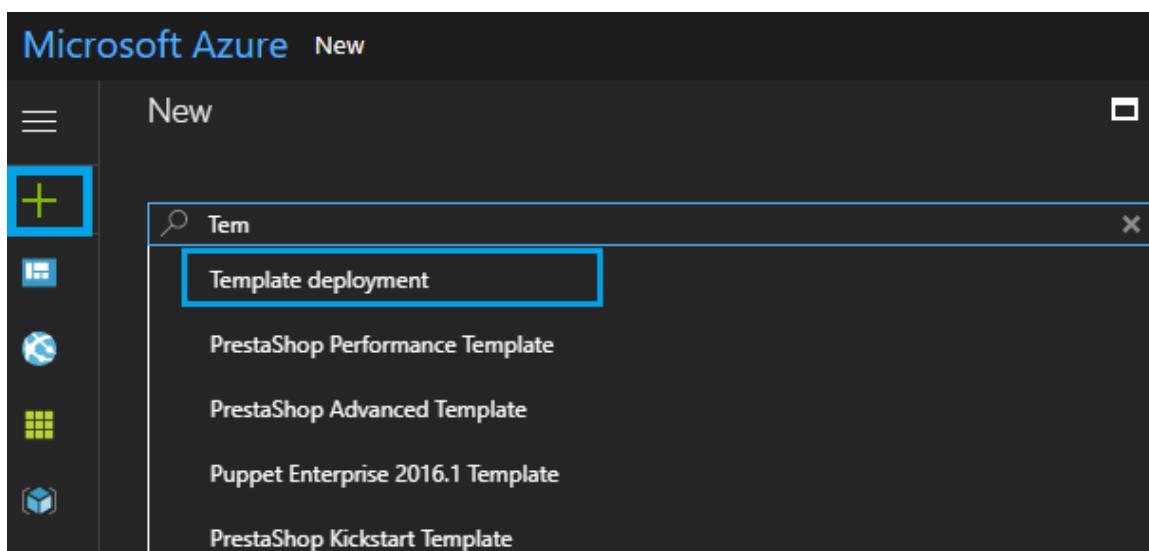
Click on below Git hub repo url

<https://github.com/sysgain/iot-automation/tree/sysgaiiot>

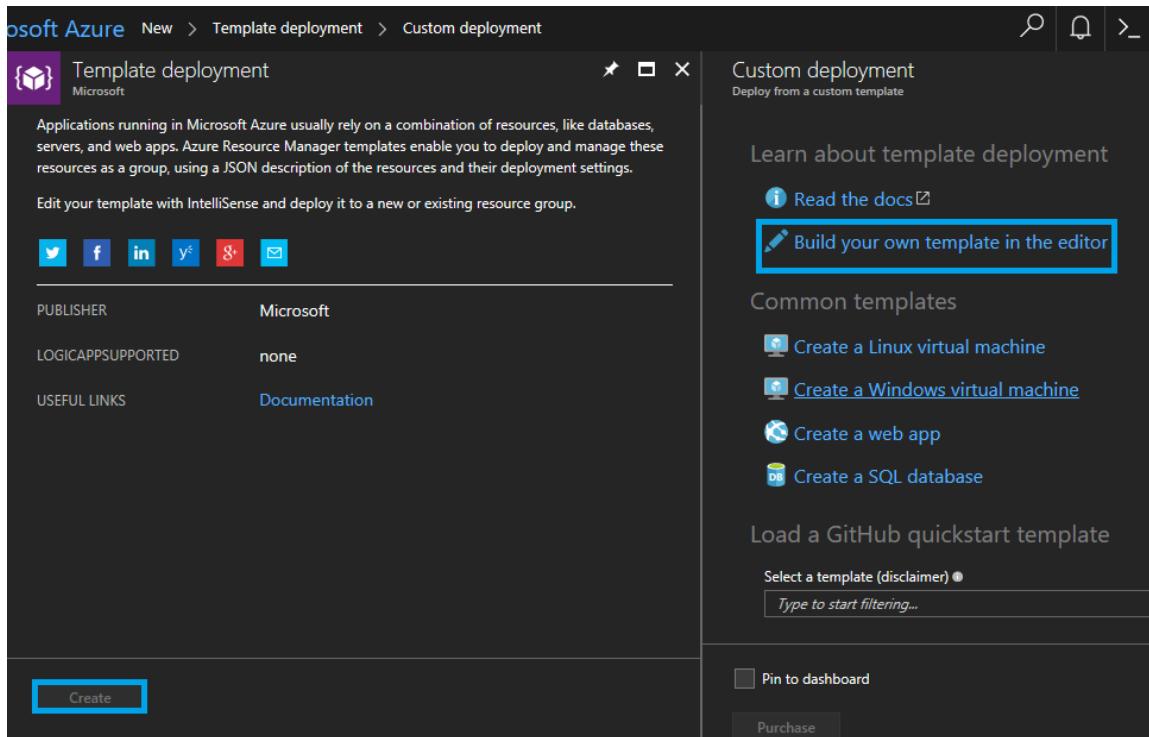
Take the [main-template.json](#) raw

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**.

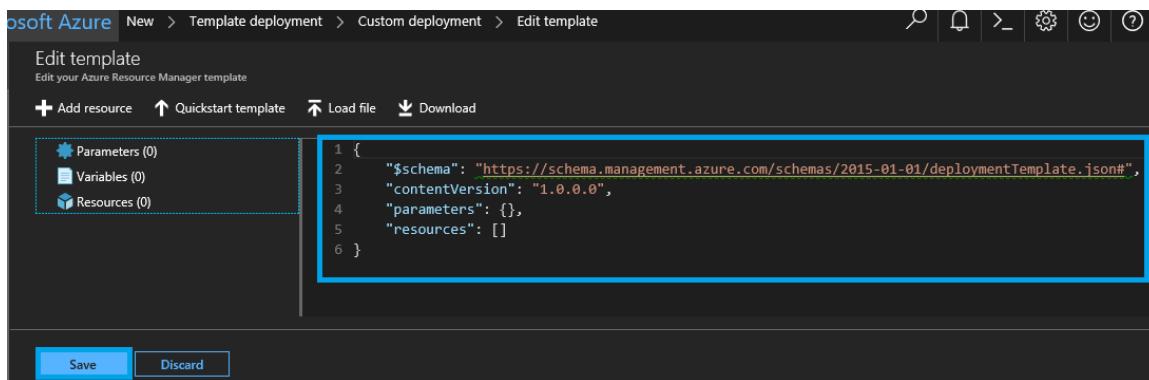


- Click on **create** and click on **Build your own Template**.



The screenshot shows the Microsoft Azure portal interface. On the left, a sidebar displays 'Template deployment' by Microsoft with links for social sharing (Twitter, Facebook, LinkedIn, YouTube, Google+, Email). Below this, publisher information is shown: PUBLISHER Microsoft, LOGICAPP SUPPORTED none, and USEFUL LINKS Documentation. At the bottom of the sidebar is a 'Create' button. On the right, the 'Custom deployment' blade is open, titled 'Custom deployment Deploy from a custom template'. It includes sections for 'Learn about template deployment' (with a 'Read the docs' link), 'Build your own template in the editor' (which is highlighted with a blue border), 'Common templates' (with links to Create a Linux virtual machine, Create a Windows virtual machine, Create a web app, and Create a SQL database), and 'Load a GitHub quickstart template' (with a search bar and a 'Pin to dashboard' button). A 'Purchase' button is also visible at the bottom of the blade.

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



The screenshot shows the 'Edit template' page in the Microsoft Azure portal. The top navigation bar includes 'New', 'Template deployment', 'Custom deployment', and 'Edit template'. Below the navigation, there's a toolbar with 'Add resource', 'Quickstart template', 'Load file', and 'Download'. The main area contains a sidebar with 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main content area displays the JSON template code:

```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5   "resources": []
6 }

```

At the bottom of the page are 'Save' and 'Discard' buttons.

- 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



Chef User Last Name ●	<input type="text" value="user"/>
Chef User Email ●	<input type="text" value="chefuser@microsoft.com"/>
Chef Org Short Name ●	<input type="text" value="cheforg"/>

TERMS AND CONDITIONS

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

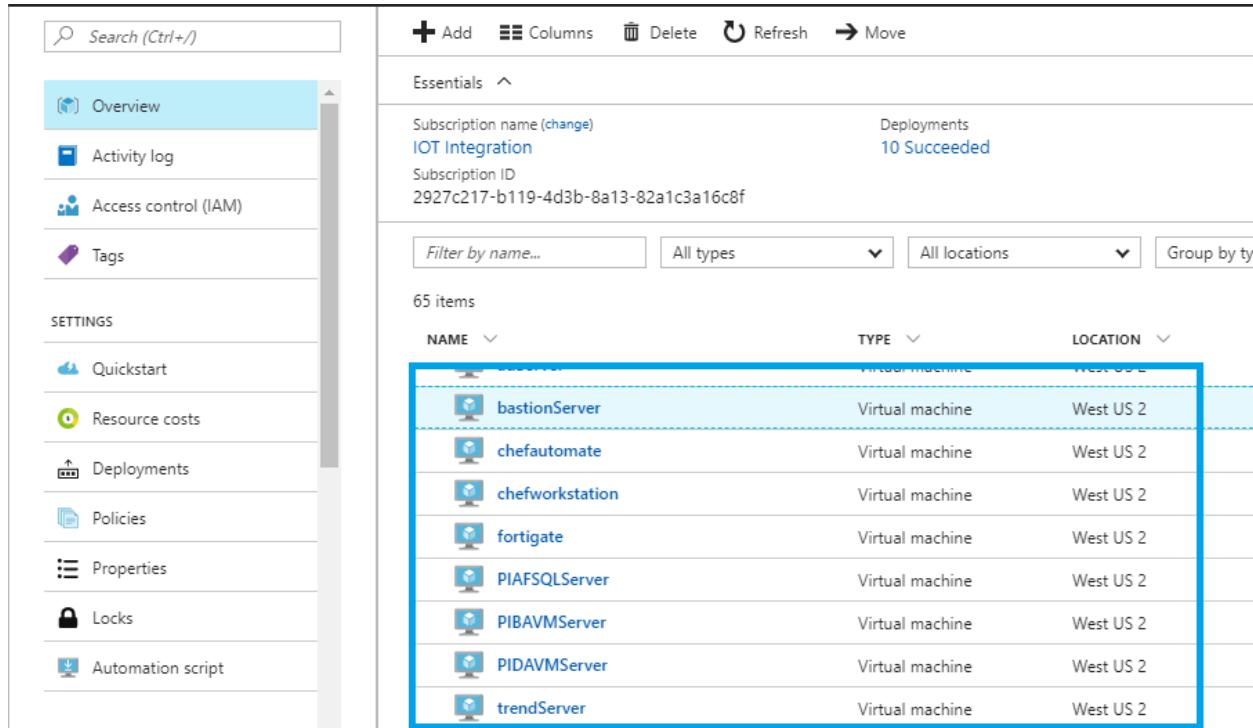
I agree to the terms and conditions stated above

Pin to dashboard

Purchase

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.



The screenshot shows the Azure portal interface for managing resources. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, SETTINGS (Quickstart, Resource costs, Deployments, Policies, Properties, Locks, Automation script), and a search bar at the top. The main area displays resource details for a specific resource group. At the top right, there are buttons for Add, Columns, Delete, Refresh, and Move. Below that, it shows the Subscription name (IOT Integration), Deployment status (10 Succeeded), and Subscription ID (2927c217-b119-4d3b-8a13-82a1c3a16c8f). A filter bar allows filtering by name, type, location, and grouping. The table lists 65 items, specifically 7 virtual machines, all located in West US 2. The virtual machines listed are: bastionServer, chefautomate, chefworkstation, fortigate, PIAFSQLServer, PIBAVMServer, PIDAVMServer, and trendServer. The entire list of VMs is highlighted with a blue border.

NAME	TYPE	LOCATION
bastionServer	Virtual machine	West US 2
chefautomate	Virtual machine	West US 2
chefworkstation	Virtual machine	West US 2
fortigate	Virtual machine	West US 2
PIAFSQLServer	Virtual machine	West US 2
PIBAVMServer	Virtual machine	West US 2
PIDAVMServer	Virtual machine	West US 2
trendServer	Virtual machine	West US 2

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.

Outputs

ADMINUSERNAME	adminuser	
BASTIONFQDN	bastionserverstnh6.southindia.cloudapp.azure.com	
ADSERVERIPADDRESS	10.0.1.4	
PIAFSQLSERVERIPADDRESS	10.0.1.5	
PIBASERVERIPADDRESS	10.0.1.11	
WORKSTATIONFQDN	wsclientsnh6.southindia.cloudapp.azure.com	
CHEFAUTOMATEIPADDRESS	10.0.1.6	
CHEFAUTOMATELOGINUSERN...	adminuser	
TRENDIPADDRESS	10.0.1.10	
TRENDWEBUIUSERNAME	adminuser	
SPLUNKIPADDRESS	10.0.1.8	



SPLUNKWEBUIUSERNAME	admin	
FORTIGATEFQDN	fortigatestnh6	
AZURESQLENDPOINT	sqlserverstnh6.database.windows.net	
AZURESQLDBNAME	azuredb	
AZURESQLUSERNAME	sqluser	
WINDOWSSQLUSERNAME	sqluser	
WEBJOBSTOREAGEACCNTNAME	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.

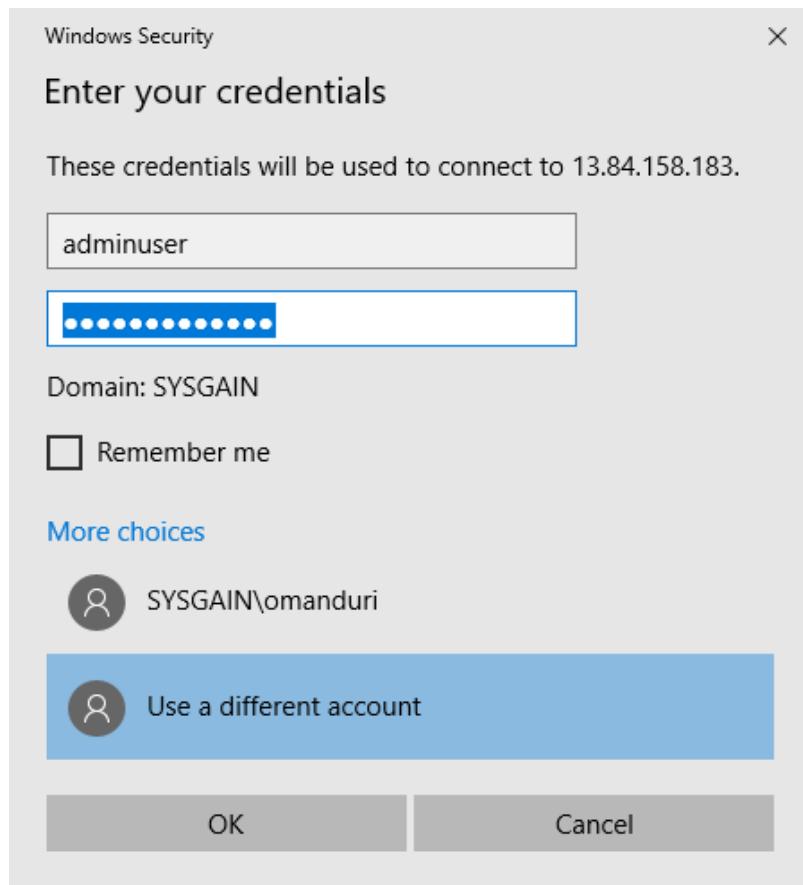
Splunk Enterprise: Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device.

7.1. Dynatrace

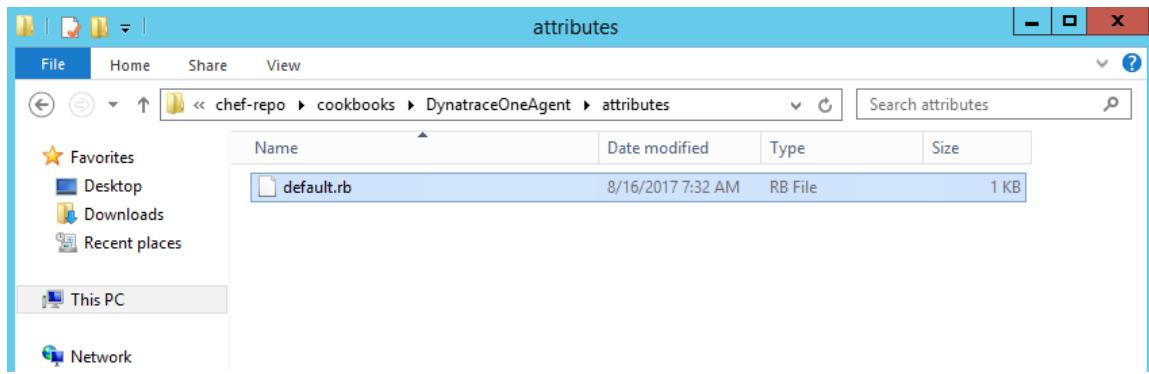
1. Log in to the **Chef Workstation** using the workstationFQDN provided in the output section.



2. Enter the credentials provided in the output section.

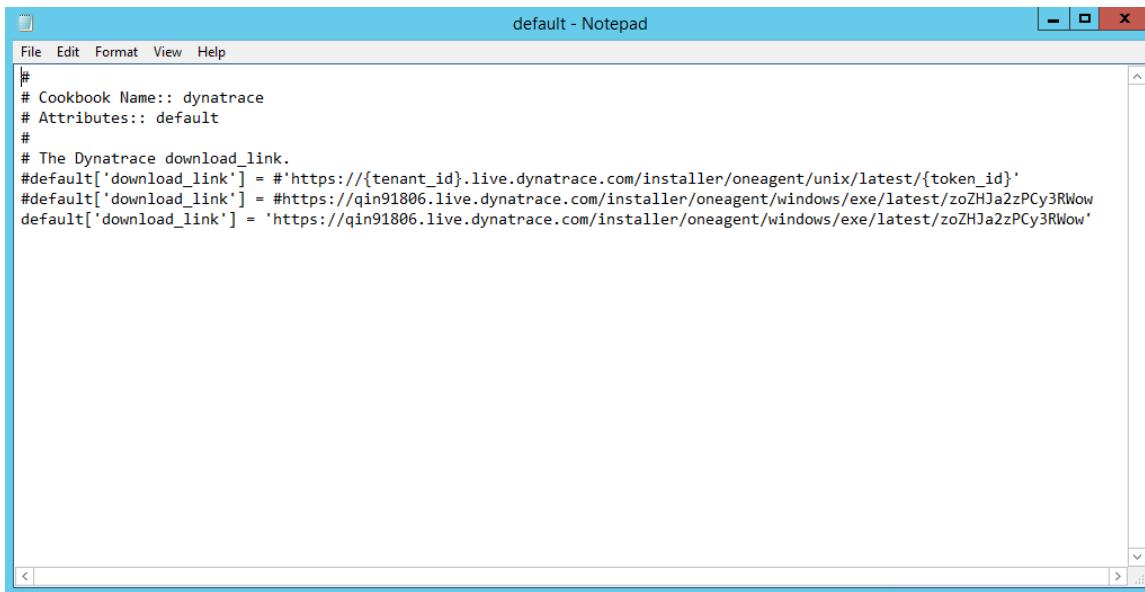


2. After logging in, navigate to **C:\Users\chef-repo\cookbooks\DynatraceOneAgent\attributes** and open the **default.rb** file.

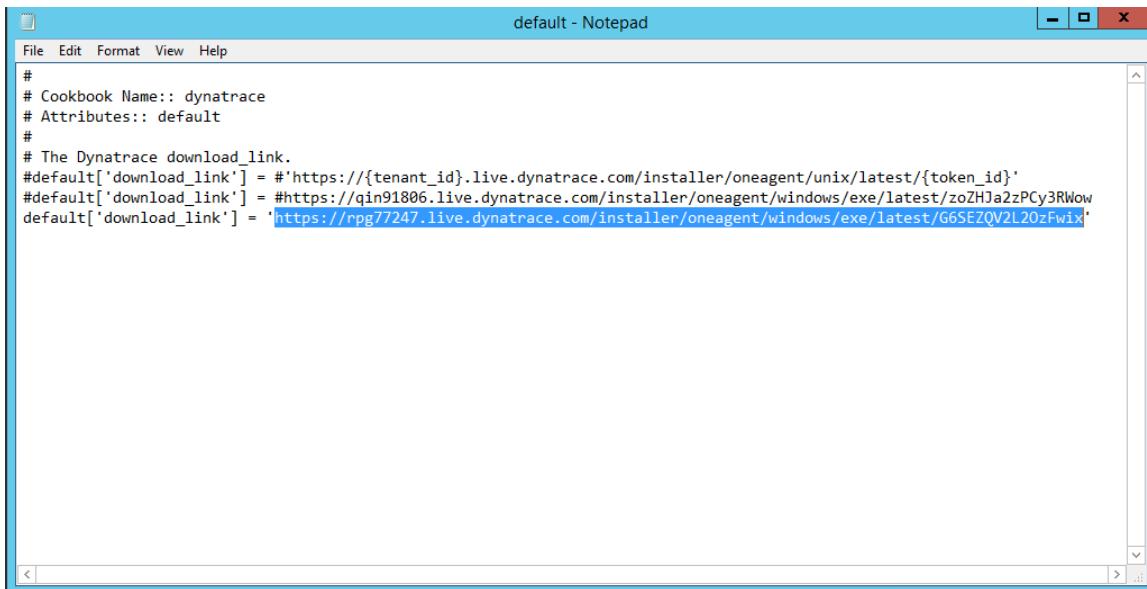


3. Add the new unique url:

<https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix> as the last link and **save** the file.

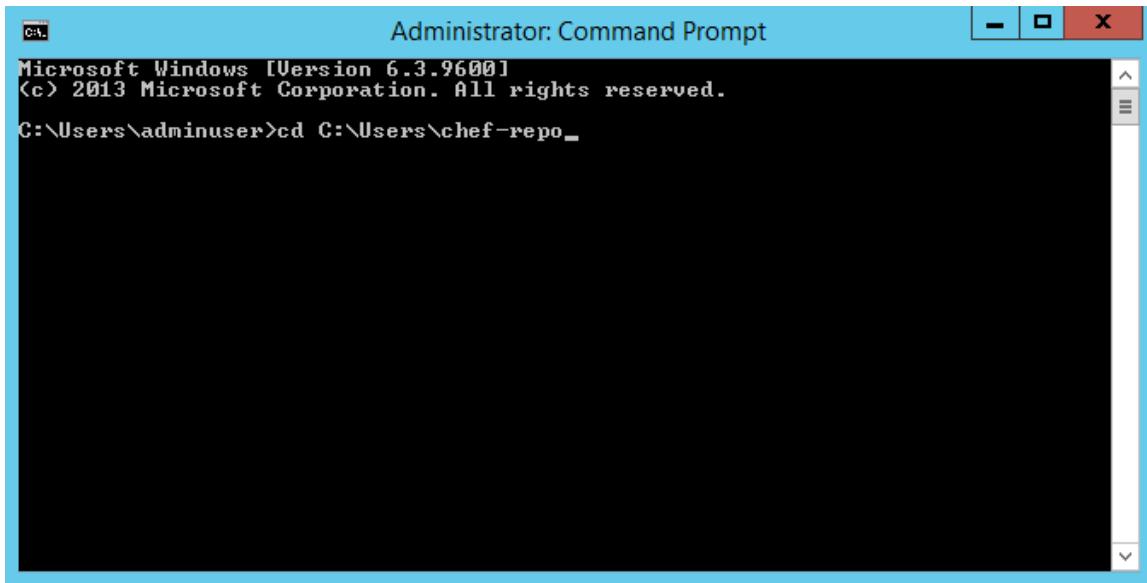


```
#  
# Cookbook Name:: dynatrace  
# Attributes:: default  
#  
# The Dynatrace download_link.  
#default['download_link'] = #'https://{{tenant_id}}.live.dynatrace.com/installer/oneagent/unix/latest/{{token_id}}'  
#default['download_link'] = #'https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow'  
default['download_link'] = 'https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow'
```



```
#  
# Cookbook Name:: dynatrace  
# Attributes:: default  
#  
# The Dynatrace download_link.  
#default['download_link'] = #'https://{{tenant_id}}.live.dynatrace.com/installer/oneagent/unix/latest/{{token_id}}'  
#default['download_link'] = #https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow  
default['download_link'] = 'https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L20zFwix'
```

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



```
Administrator: Command Prompt  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Users\adminuser>cd C:\Users\chef-repo\
```

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

knife cookbook upload DynatraceOneAgent

```
C:\> Administrator: Command Prompt  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Users\adminuser>cd C:\Users\chef-repo  
C:\Users\chef-repo>cd cookbooks_
```

```
C:\> Administrator: Command Prompt  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Users\adminuser>cd C:\Users\chef-repo  
C:\Users\chef-repo>cd cookbooks  
C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent  
Uploading DynatraceOneAgent [0.1.0]  
Uploaded 1 cookbook.  
C:\Users\chef-repo\cookbooks>_
```

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

knife client list

Administrator: Command Prompt

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\adminuser>cd C:\Users\chef-repo

C:\Users\chef-repo>cd cookbooks

C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserver2yo2.southcentralus.cloudapp.azure.com
orguser-validator
pidadnsz7yo2.southcentralus.cloudapp.azure.com
wsclientz7yo2.southcentralus.cloudapp.azure.com

C:\Users\chef-repo\cookbooks>_

```

- 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

Administrator: Command Prompt

```

C:\Users\adminuser>cd C:\Users\chef-repo

C:\Users\chef-repo>cd cookbooks

C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

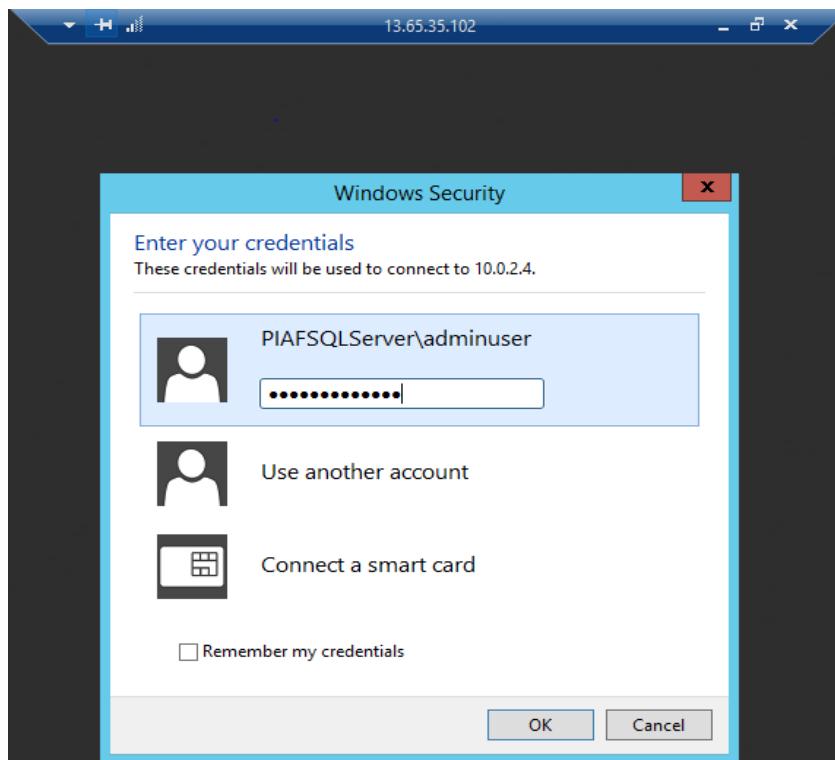
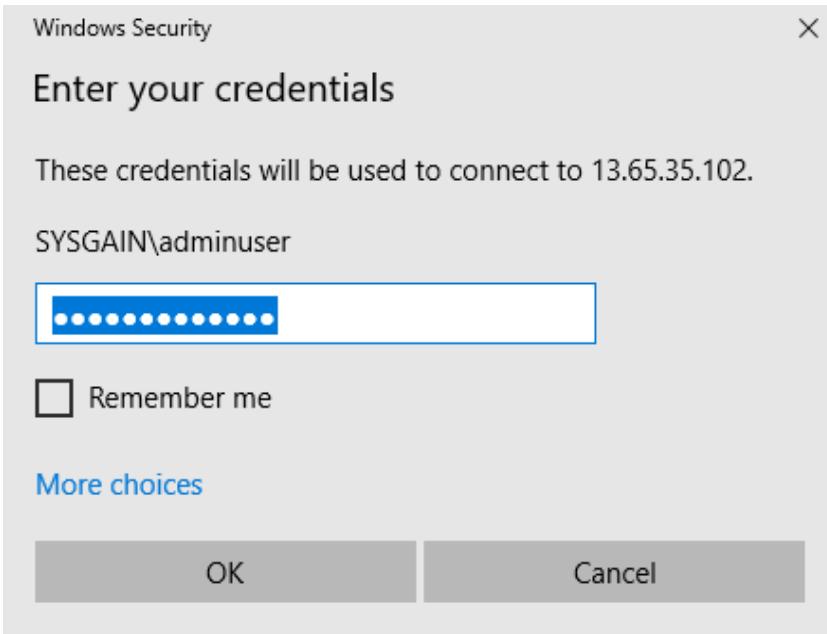
C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserver2yo2.southcentralus.cloudapp.azure.com
orguser-validator
pidadnsz7yo2.southcentralus.cloudapp.azure.com
wsclientz7yo2.southcentralus.cloudapp.azure.com

C:\Users\chef-repo\cookbooks>knife node run_list add 10.0.2.4 DynatraceOneAgent
10.0.2.4:
  run_list:
    recipe[git]
    recipe[audit]
    recipe[DynatraceOneAgent]

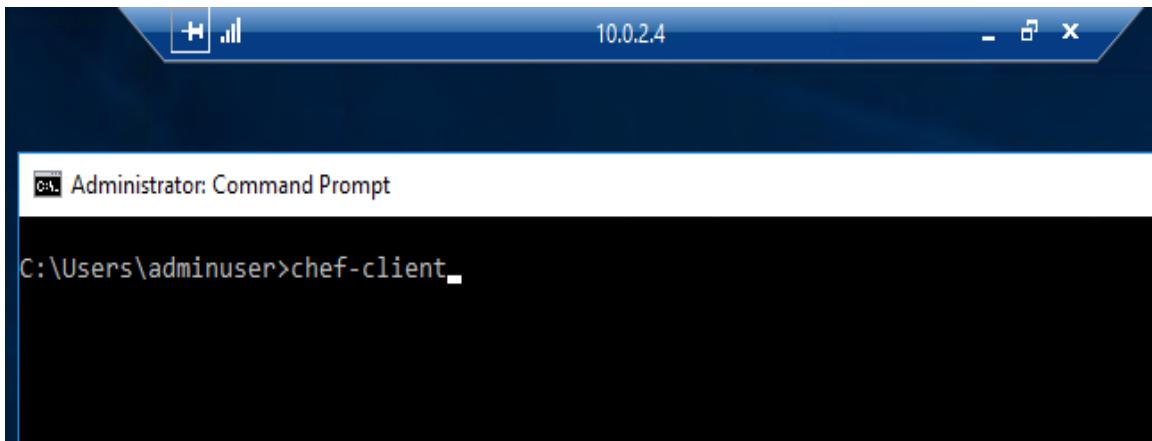
C:\Users\chef-repo\cookbooks>_

```

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



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



Administrator: Command Prompt

```
C:\Users\admininuser>chef-client
```

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

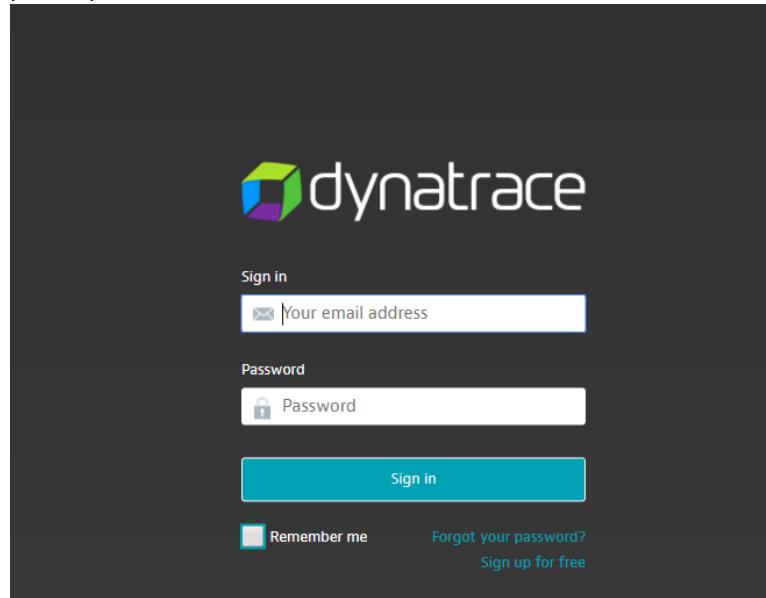
```
- install version latest of package DynatraceOneAgent
* windows_service[Dynatrace OneAgent] action restart[2017-08-16T14:10:56+00:00] INFO: Processing windows_service[Dynatrace OneAgent] action restart (DynatraceOneAgent::oneagent-windows line 28)
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace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

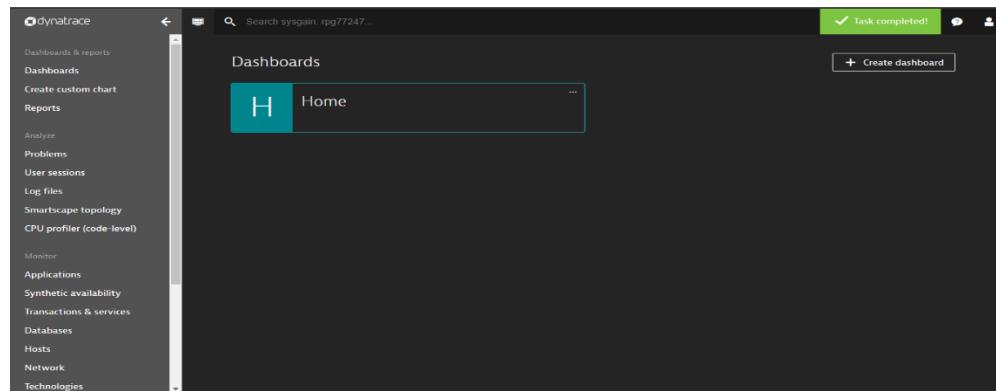
- restart service windows_service[Dynatrace OneAgent]
[2017-08-16T14:11:09+00:00] INFO: Chef Run complete in 22.297144 seconds

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/windows-baseline"}]
```

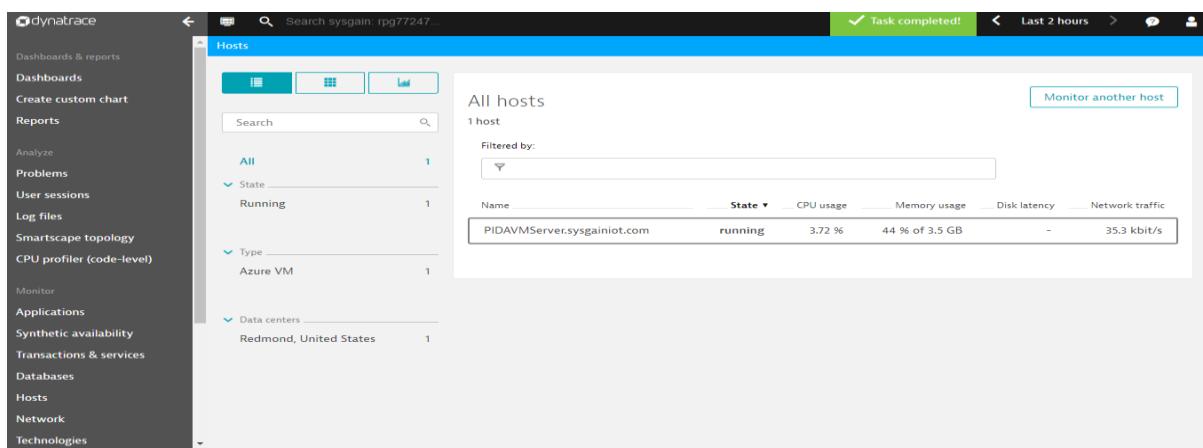
11. Go to the Dynatrace dashboard using the following URL: <https://www.dynatrace.com/>

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





- 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.

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

The screenshot shows the Dynatrace web interface at <https://sly90549.live.dynatrace.com/#deploymentstatus>. The left sidebar includes options like CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main content area displays the 'Deployment status' for 'adServer.sysgainiot.com' (IP address: 10.0.1.4). It shows 6 hosts. For the selected host, it indicates that Dynatrace OneAgent is up-to-date on version 1.125. Under 'Automatically detected processes that support Service insights:', there are three entries: Microsoft.ActiveDirectory.WebServices.exe (Process isn't monitored, with a note to restart for full visibility), WaAppAgent.exe (Process isn't monitored, with a note to restart for full visibility), and WindowsAzureGuestAgent.exe (Process isn't monitored, with a note to restart for full visibility). Each process entry has a 'Disable monitoring' button.

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

The screenshot shows the Dynatrace web interface at <https://sly90549.live.dynatrace.com/#deploymentstatus>. The left sidebar includes options like CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main content area displays the 'Deployment status' for 'RD00155DA9BEC5' (IP address: 10.69.152.36). It shows 6 hosts. For the selected host, it indicates that the host is monitored. Under 'Automatically detected processes that support Service insights:', there are five IIS app pools listed: EnergyManagementScheduler.WebJob.exe (Process is monitored), apiservergop4o (Process is monitored), webiotivivek (Process is monitored), ~apiservergop4o (Process is monitored), and ~webiotivivek (Process is monitored). Each app pool has a 'Disable monitoring' button.

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.

Screenshot of the Dynatrace interface showing the host details for PIDAVMServer.sysgainiot.com. The left sidebar shows various monitoring categories like Dashboards & reports, Reports, and Applications. The main panel displays the host's properties, uptime (1 day 1 hour 54 minutes), and a summary card showing 100% Availability with 0 min total downtime. A CPU usage chart shows 0.29% usage over the last hour. A list of running processes is also shown.

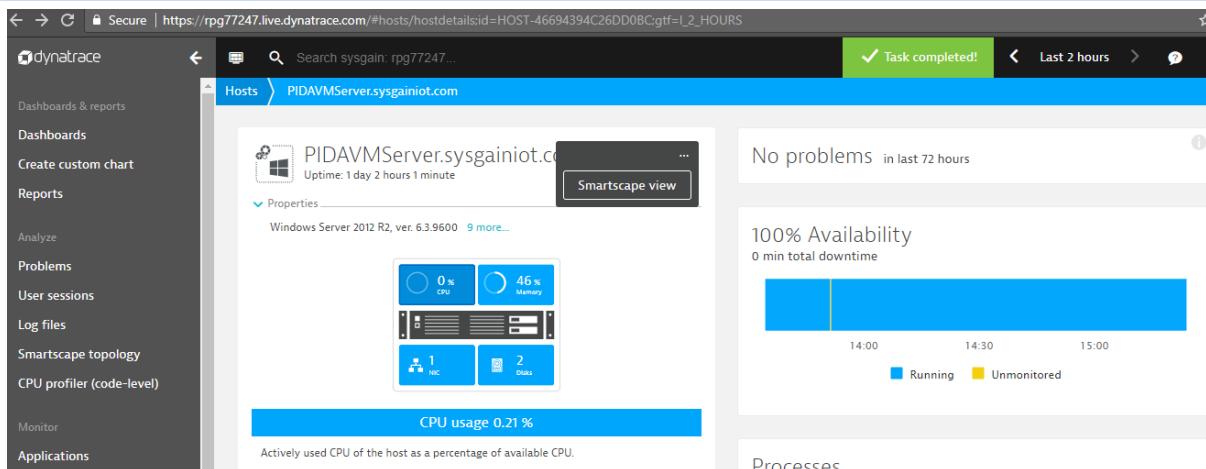
15. Click on “**All processes**”, to view the process details running on the host.

Screenshot of the Dynatrace interface showing the list of processes running on the host. The left sidebar is identical to the previous screenshot. The main panel lists 15 processes, each with its name, type, CPU usage, memory usage, traffic, retransmissions, and connectivity status. Notable processes include Deep Security Agent, OneAgent log analytics, Windows System, and various Dynatrace and .NET services.

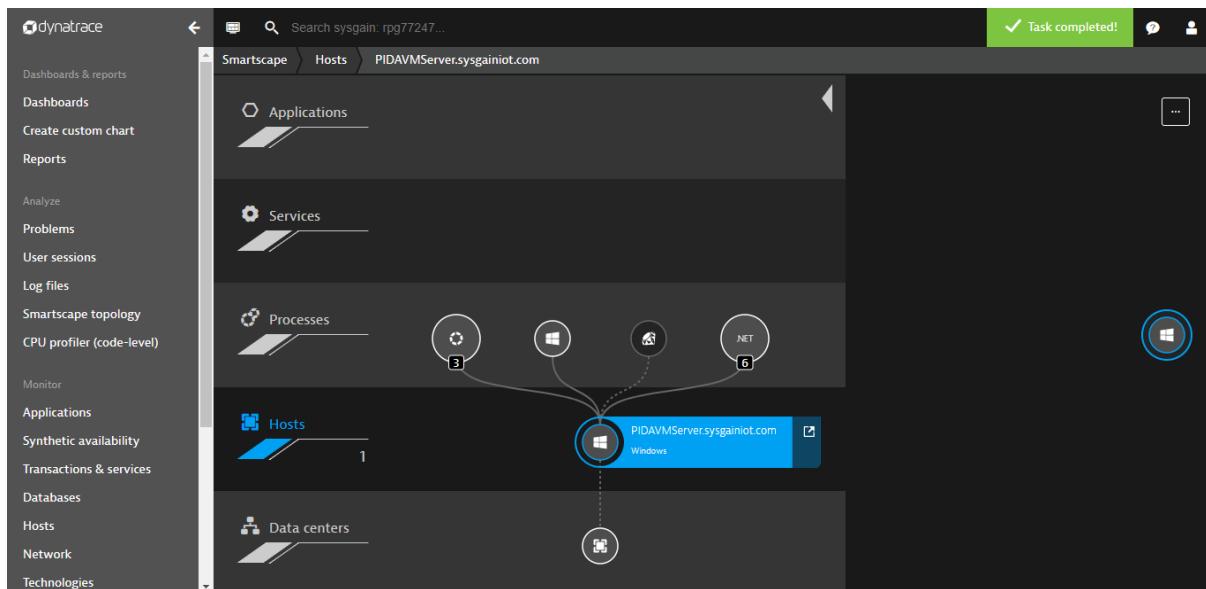
Process	Type	CPU	Memory	Traffic	Retransmissions	Connectivity
Deep Security Agent	Other	4.51 %	41.6 MB	-	-	-
OneAgent log analytics	Dynatrace	0.1 %	15.1 MB	4.74 kbit/s	0 %	100 %
Windows System	Windows	0.1 %	617 MB	4.84 kbit/s	3.6 %	100 %
ServerManager.exe	.NET	0 %	69.1 MB	-	-	-
OneAgent network monitoring	Dynatrace	0 %	14.6 MB	-	-	-
Remote Desktop Connection	Other	0 %	88.3 MB	1.87 kbit/s	0 %	100 %
piaflink.exe	.NET	0 %	58.2 MB	1.47 kbit/s	0 %	100 %
OneAgent monitoring extensions	Dynatrace	0 %	35.4 MB	-	-	-
oneagentupdater.exe	Other	0 %	0 B	-	-	-
WindowsAzureTelemetryService.exe	.NET	0 %	50.6 MB	-	-	-
SMTHost.exe	.NET	0 %	116 MB	-	-	-
chef-client	Ruby	0 %	0 B	-	-	-
WaAppAgent.exe	.NET	0 %	44.5 MB	358 bit/s	0 %	100 %

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.



The screenshot shows the Dynatrace interface for a host named PIDAVMServer.sysgainiot.com. The left sidebar includes options like Dashboards & reports, Dashboards, Create custom chart, Reports, Analyze, Problems, User sessions, Log files, Smartscape topology, CPU profiler (code-level), Monitor, and Applications. The main panel displays the host's properties, including its name, uptime (1 day 2 hours 1 minute), and version (Windows Server 2012 R2, ver. 6.3.9600). It also shows real-time monitoring metrics: 0% CPU and 46% Memory. A large blue bar indicates CPU usage at 0.21%. To the right, a summary card shows "No problems in last 72 hours" and "100% Availability" with 0 min total downtime. A timeline from 14:00 to 15:00 shows the status: Running (blue) and Unmonitored (yellow).



The screenshot shows the Dynatrace Smartscape topology view for the same host. The left sidebar lists categories such as Applications, Services, Processes, Hosts, and Data centers. The main area displays a network diagram where the host is connected to various application components. A Windows icon is highlighted, indicating the specific host node in the topology.

7.1.1. Installing Dynatrace oneagent To Web Application (PaaS Environment)

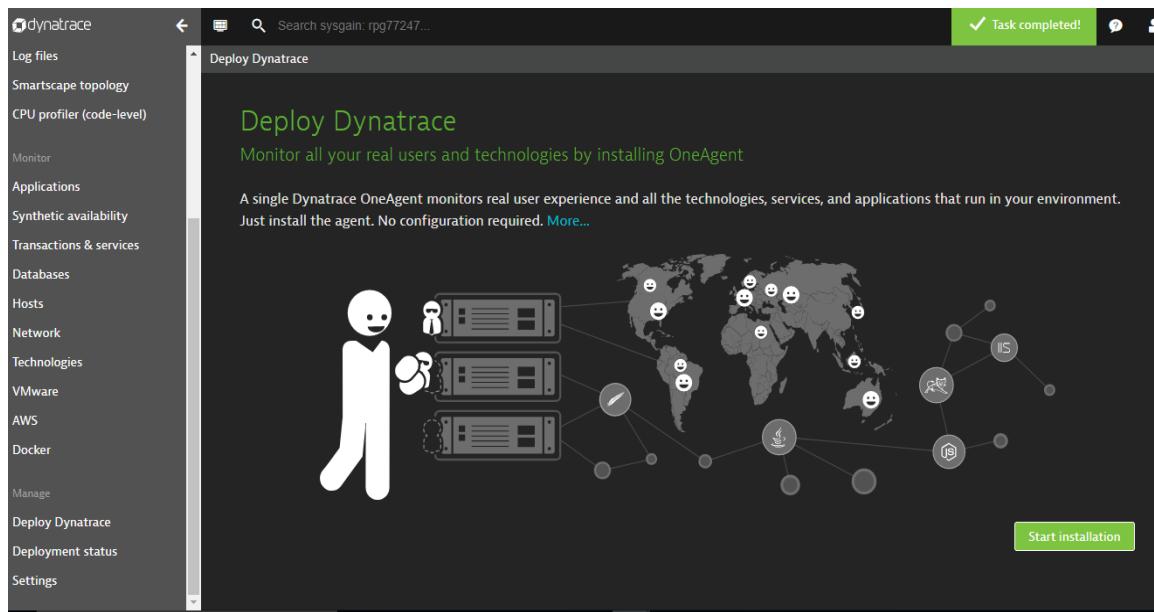
Azure Web Apps is a service provided by Microsoft Azure that gives you the option of deploying and auto-scaling applications and services. Using a predefined Azure site extension, you can modify your deployment by supplying additional resources or packages.

Generate a PaaS token:

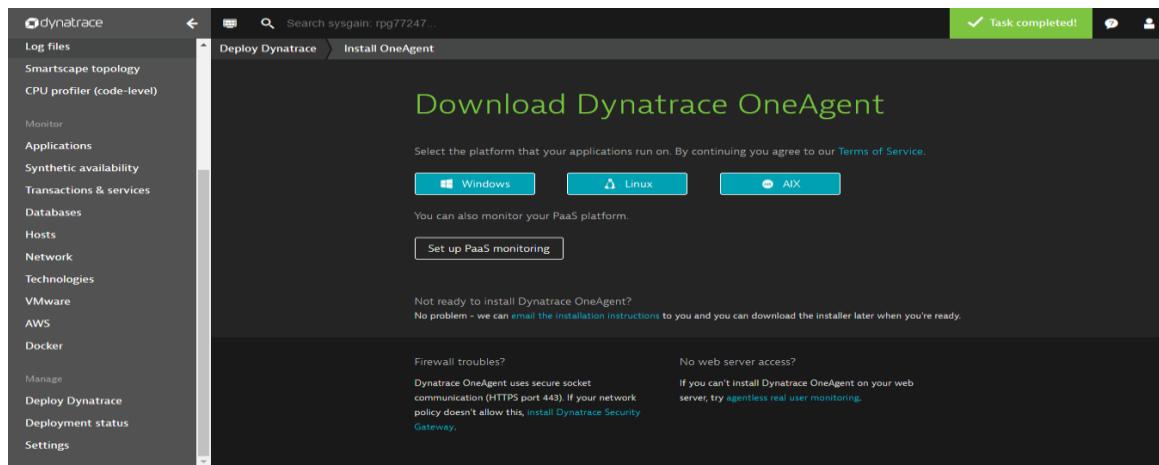
The first step is to get your environment ID and generate a PaaS token for your Dynatrace environment. This information is required so we can map your Azure account to your Dynatrace account.

To get your Dynatrace environment ID and PaaS token:

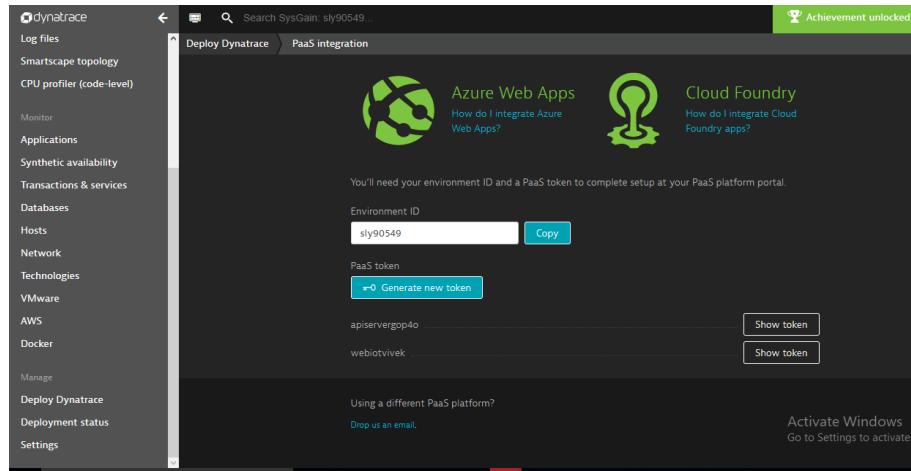
1. Login with your [Dynatrace account](#).
2. Select Deploy Dynatrace from the navigation menu.



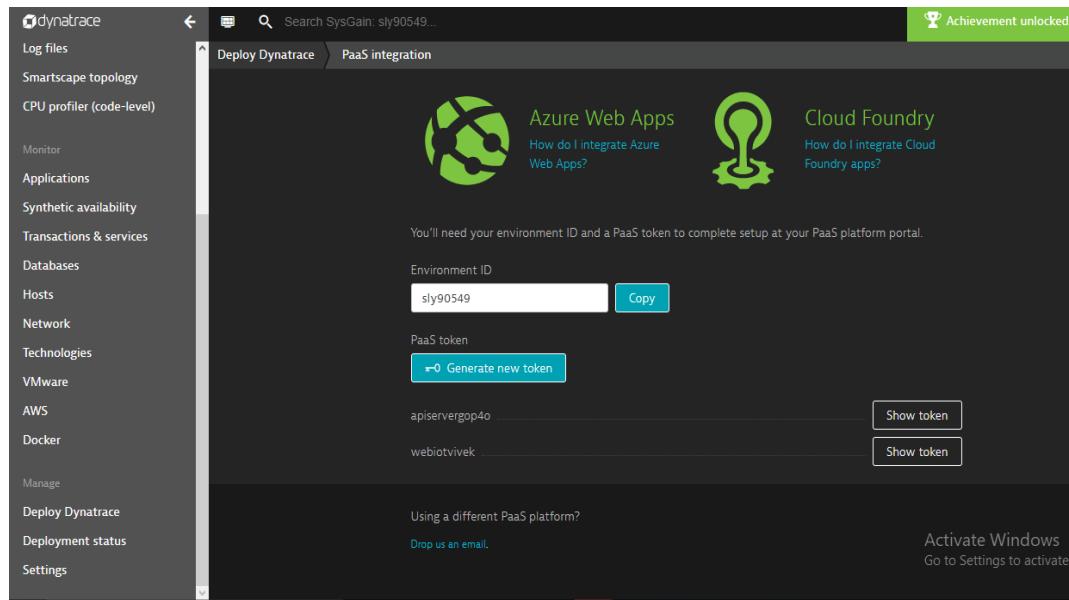
3. Click **Setup PaaS monitoring**.



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.

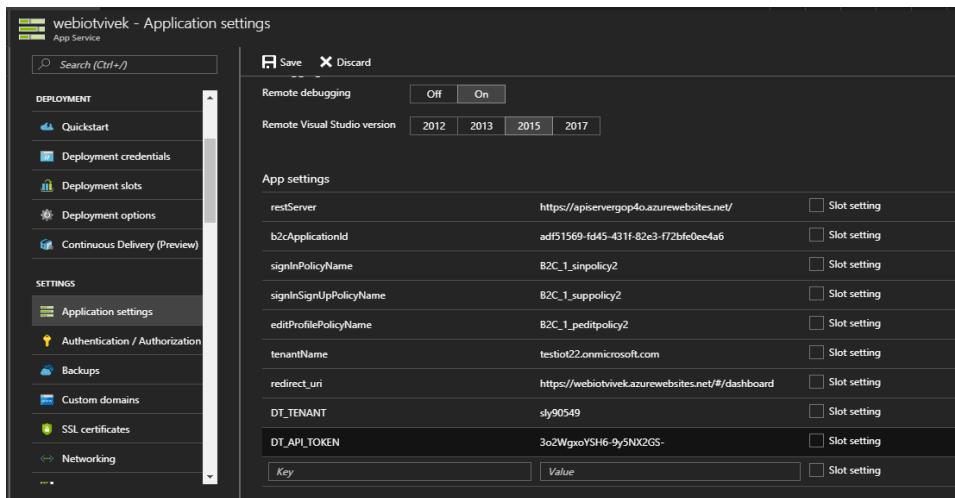


6. Type in a meaningful name for your PaaS token. A meaningful token name might be the name of the PaaS platform you want to monitor (for example: azure, cloud-foundry, or openshift). To view and manage your existing PaaS tokens, go to **Settings > Integration > Platform as a Service**.

- In the screenshots, we have now generated a PaaS 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

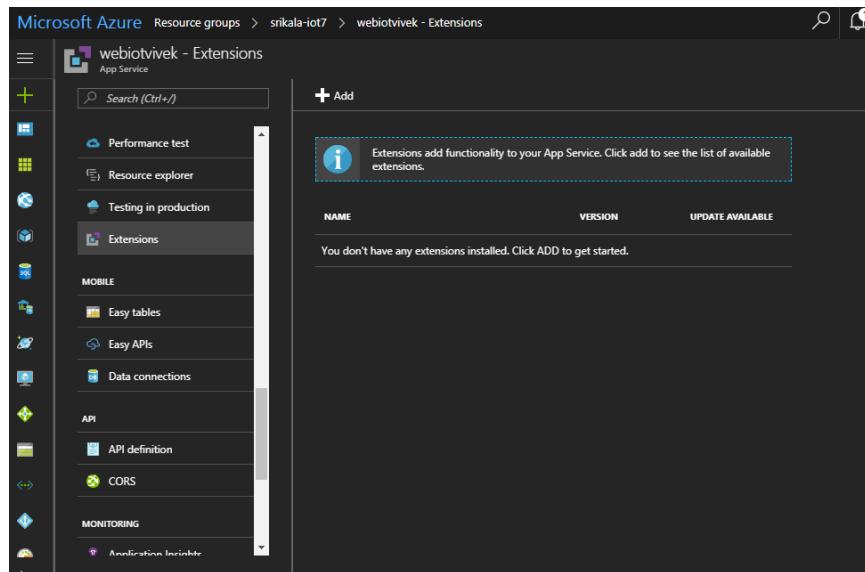
1. Now, open **portal.azure.com** in a new browser window.
2. Navigate to the web app in the resource group you want to monitor.
3. From **Settings**, select **Application Settings**. Then, scroll down to the App Settings area and add two new **Key/Value** pairs:
4. **DT_TENANT**: Your environment ID, 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>.



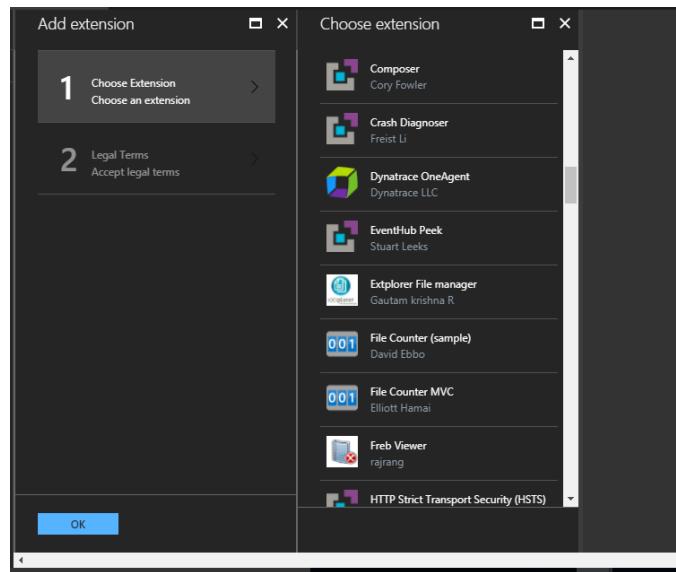
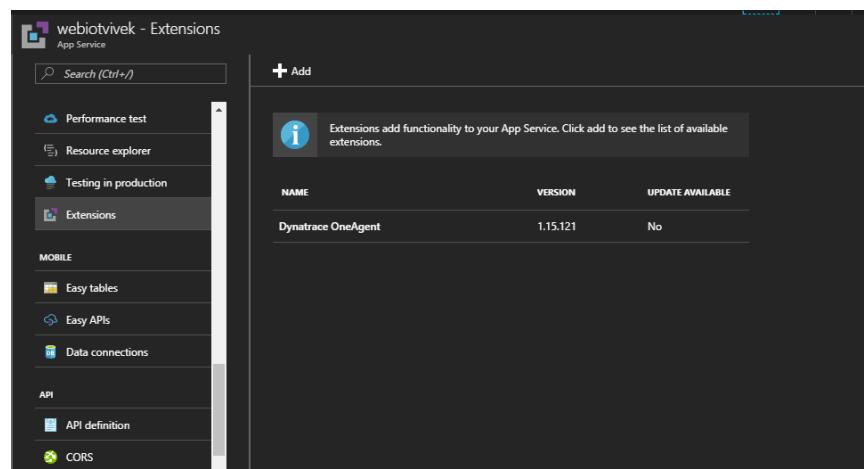
Install the Dynatrace Azure site extension

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**.



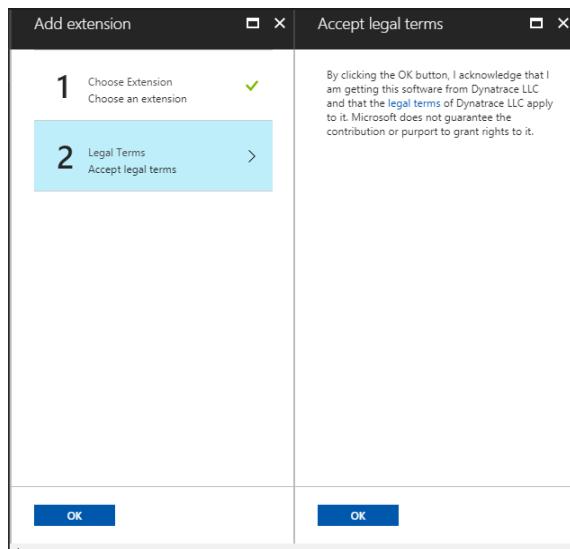
5. Scroll through the list until you find **Dynatrace OneAgent**. Note that entries are not ordered alphabetically. <https://help.dynatrace.com/images/content/infrastructure-monitoring/paas/extension.png>

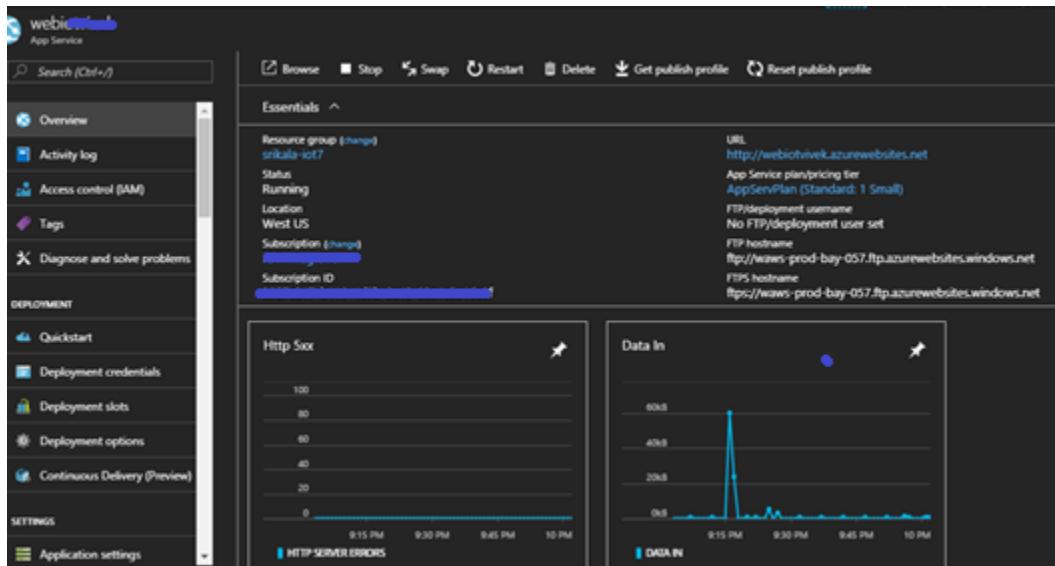
The screenshot shows the Azure portal's "Extensions" blade for the "webiotvivek" App Service. On the left, a sidebar lists various service components: Performance test, Resource explorer, Testing in production, Extensions (which is selected), and sections for MOBILE (Easy tables, Easy APIs, Data connections) and API (API definition, CORS). The main area displays a message: "Extensions add functionality to your App Service. Click add to see the list of available extensions." Below this, a table lists the available extension "Dynatrace OneAgent" with version 1.15.121 and an "UPDATE AVAILABLE" status. A "Add" button is located at the top right of the main area.

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

SysGain dashboard showing Services section. The sidebar includes links for dynatrace, CPU profiler, Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings.

The main area displays "All monitored services" with 2 services listed:

Name	Response time	Failure rate	Requests
~!webiotivek	571 ms	0 %	2 /min
webiotivek	3.6 ms	0 %	1/min

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

Application settings for webiapp - App Service. The left sidebar shows SETTINGS with Application settings selected. The main area shows App settings and Connection strings.

App settings

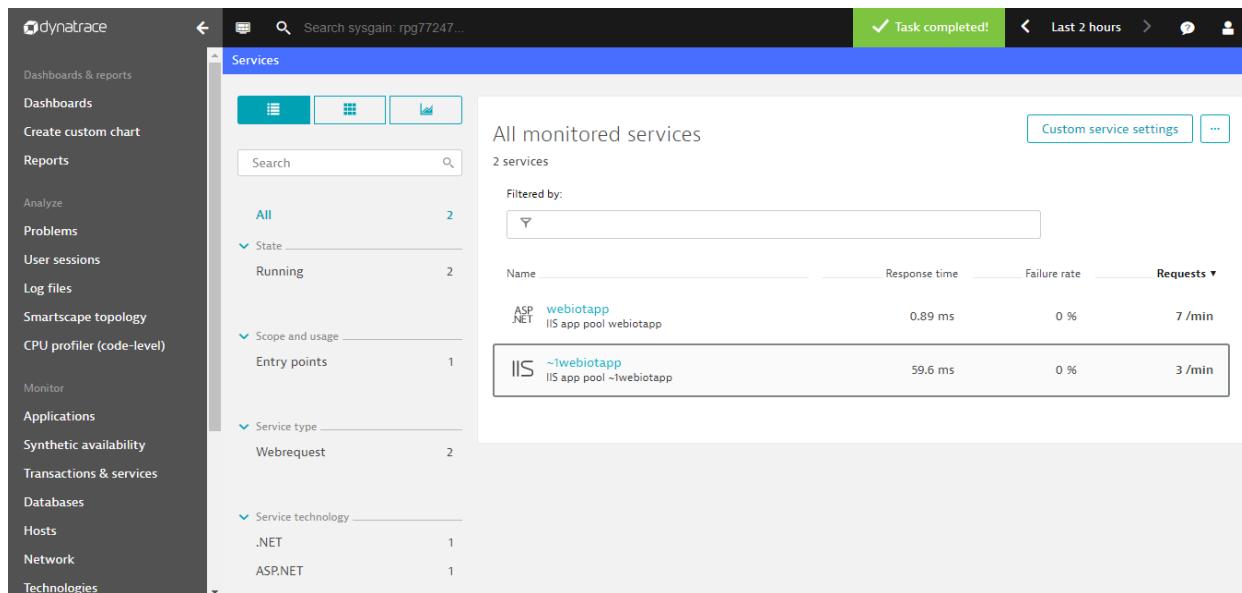
restServer	https://apiserver4yjl.azurewebsites.net/	<input type="checkbox"/> Slot setting	...
b2cApplicationId	9e82abb2-c190-4ae2-b576-7d8e63fcf3e1	<input type="checkbox"/> Slot setting	...
signInPolicyName	B2C_1_sinpolicy2	<input type="checkbox"/> Slot setting	...
signInSignUpPolicyName	B2C_1_suppolicy2	<input type="checkbox"/> Slot setting	...
editProfilePolicyName	B2C_1_peditpolicy2	<input type="checkbox"/> Slot setting	...
tenantName	testiot22.onmicrosoft.com	<input type="checkbox"/> Slot setting	...
redirect_uri	https://webiapp.azurewebsites.net/#/dashboard	<input type="checkbox"/> Slot setting	...
DT_TENANT	rpg77247	<input type="checkbox"/> Slot setting	...
DT_API_TOKEN	v81tKAGES6-77rP4LWe8H	<input type="checkbox"/> Slot setting	...

Connection strings

The connection string values are hidden. Show connection string values.

BlobConnection	< Hidden for Security >	Custom	<input type="checkbox"/> Slot setting	...
----------------	-------------------------	--------	---------------------------------------	-----

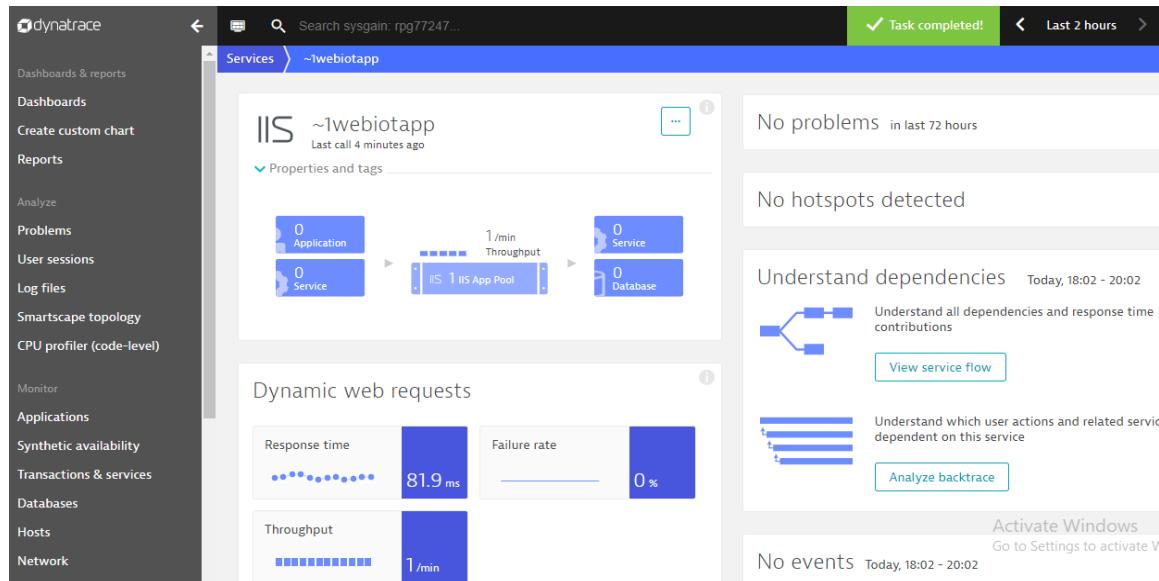
10. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added.



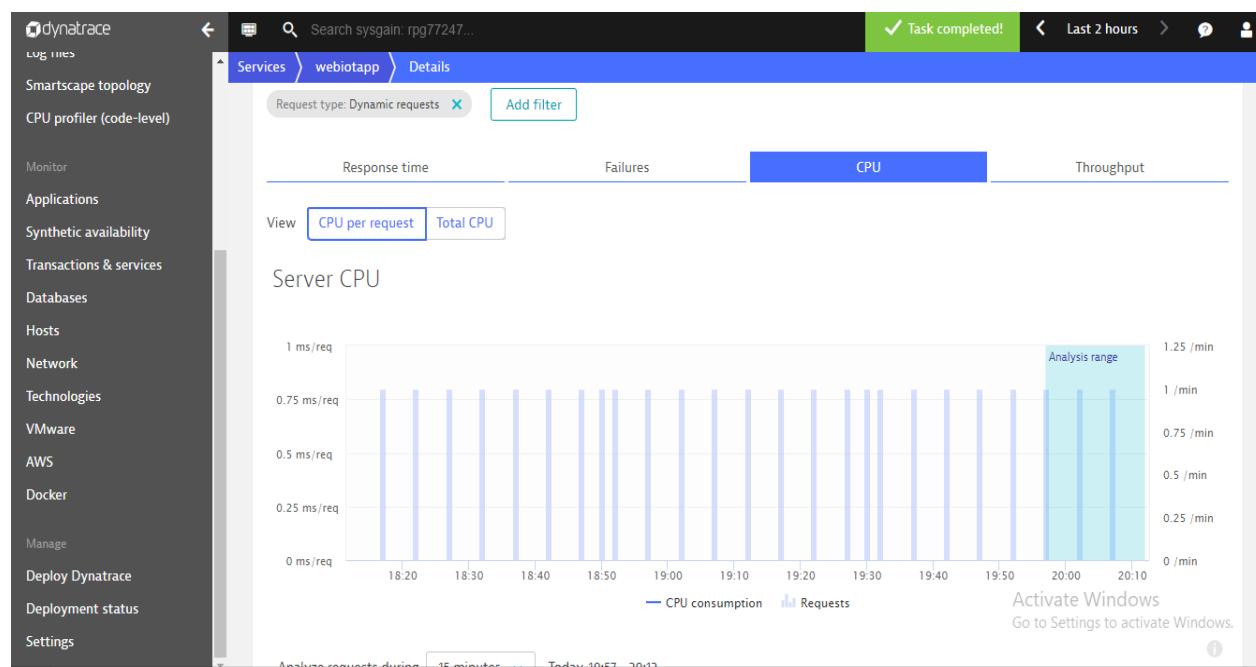
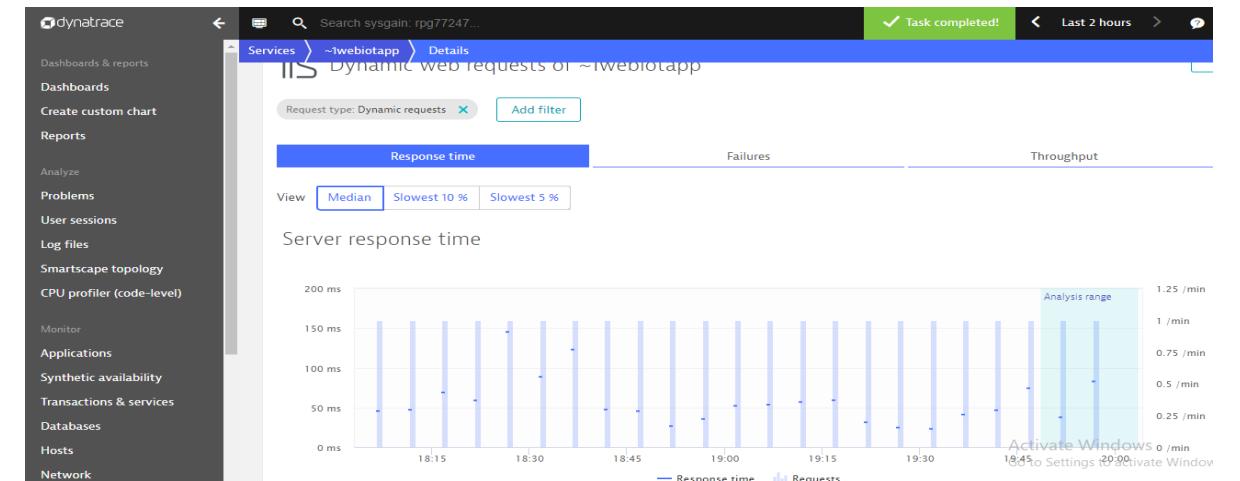
The screenshot shows the Dynatrace Services dashboard. On the left sidebar, under the "Services" section, there are filters for "Scope and usage", "Service type", and "Service technology". The main area displays "All monitored services" with 2 services listed:

Name	Response time	Failure rate	Requests
ASP .NET webiotapp	0.89 ms	0 %	7 /min
IIS ~!webiotapp	59.6 ms	0 %	3 /min

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



The screenshot shows the Dynatrace service details for "IIS ~!webiotapp". The left sidebar has a "Properties and tags" section. The main area includes a "Dynamic web requests" summary with metrics: Response time (81.9 ms), Failure rate (0 %), and Throughput (1/min). To the right, there are sections for "No problems in last 72 hours", "No hotspots detected", "Understand dependencies" (with a "View service flow" button), and "No events" (with a "Activate Windows" button).



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

Screenshot of the Sysgain interface showing the service 'webiotapp' details. The left sidebar includes options like dynatrace, log files, Smartscape topology, CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings.

The main panel displays the service flow: Application (0), Throughput (1/min), Service (0), and Database (0). It also shows 'Dynamic web requests' with metrics: Response time (1.83 ms), Failure rate (0%), CPU, and Throughput (1/min). A 'View dynamic requests' button is present.

On the right, a section titled 'Understand dependencies' shows no hotspots detected. It includes a 'View service flow' button and a 'Analyze backtrace' button. Below this is a 'No events' section with a 'View PurePaths' button.

Screenshot of the Sysgain interface showing the 'Service flow' for the 'webiotapp'. The left sidebar is identical to the previous screenshot.

The main panel shows the service flow for 'webiotapp' with a timestamp of 'Today, 18:18 - 20:18 (2 Hours)'. It includes an 'Add filter' button and a summary for 'ASP.NET webiotapp': Avg. response time (77.9 ms), Requests (26), and Failed requests (0). A 'View PurePaths' button is available.

A note below states: 'See every single request in PurePath view'. A 'show more' button is present.

The right side shows a 'No service selected' message with a note: 'Select any service in the service flow to get more details and perform deeper analysis'. A 'Activate Windows' button is at the bottom.

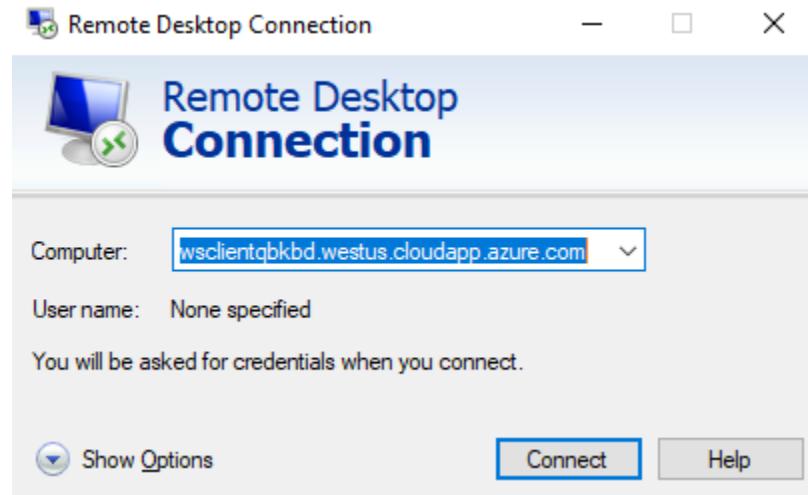
13. To understand which user actions and related services are dependent on this service, Click **Analyze backtrace**.

The screenshot shows the Sysgain Dynatrace interface. The left sidebar contains navigation links: dynatrace, Log files, Smartscape topology, CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main area displays a 'Service-level backtrace of requests to 'webiotapp'' for the period 'Today, 18:20 - 20:20 (2 Hours)'. It includes a search bar, a date range selector, and an 'Apply' button. Below this is a section titled 'Incoming requests to this service' showing a tree view with nodes: ASP .NET webiotapp IIS app pool webiotapp. A progress bar indicates '26 Requests' with '0 Failed requests'. A green banner at the top right says 'Task completed!' with a checkmark icon.

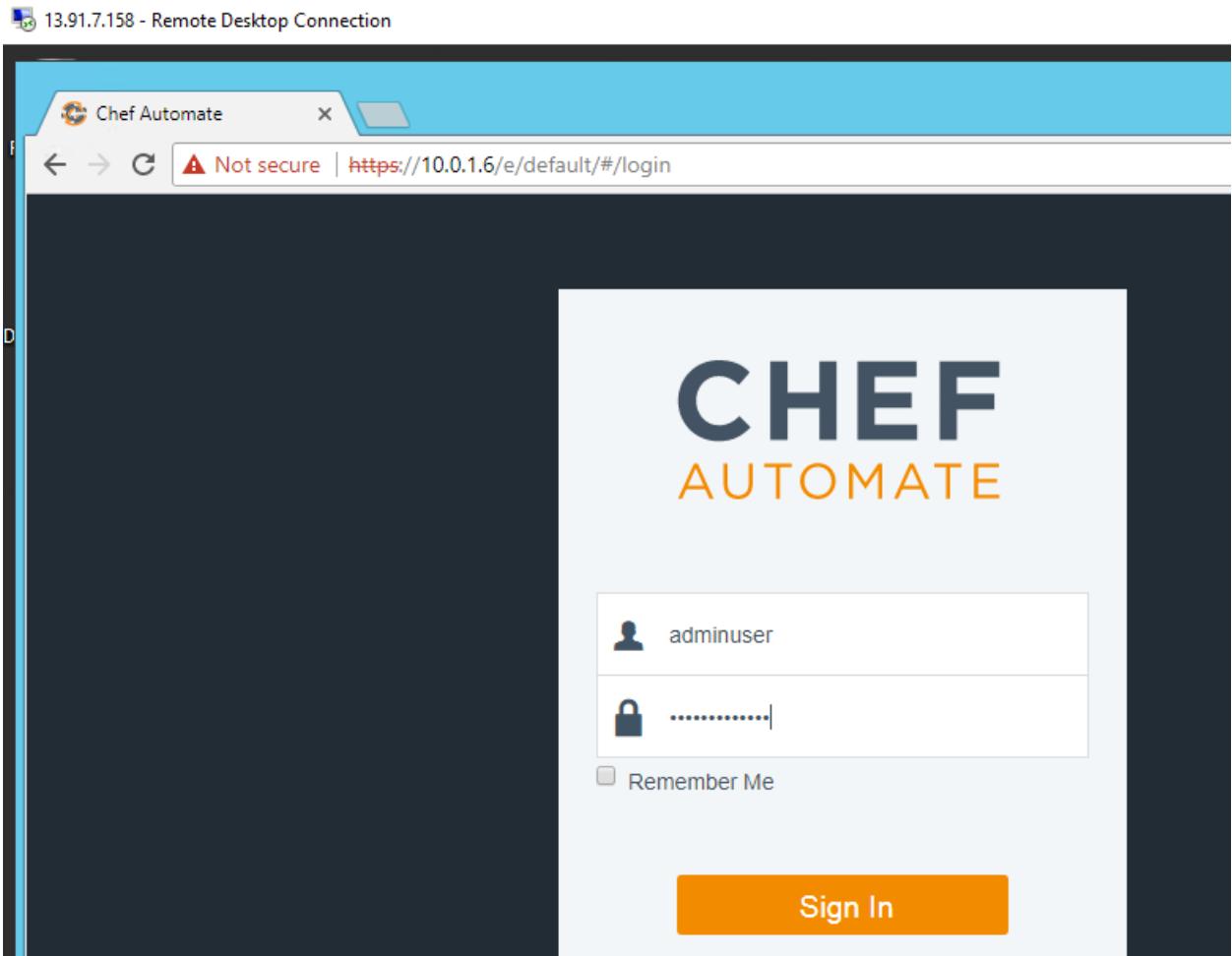
7.2. Chef Automate

To check the installed nodes status.

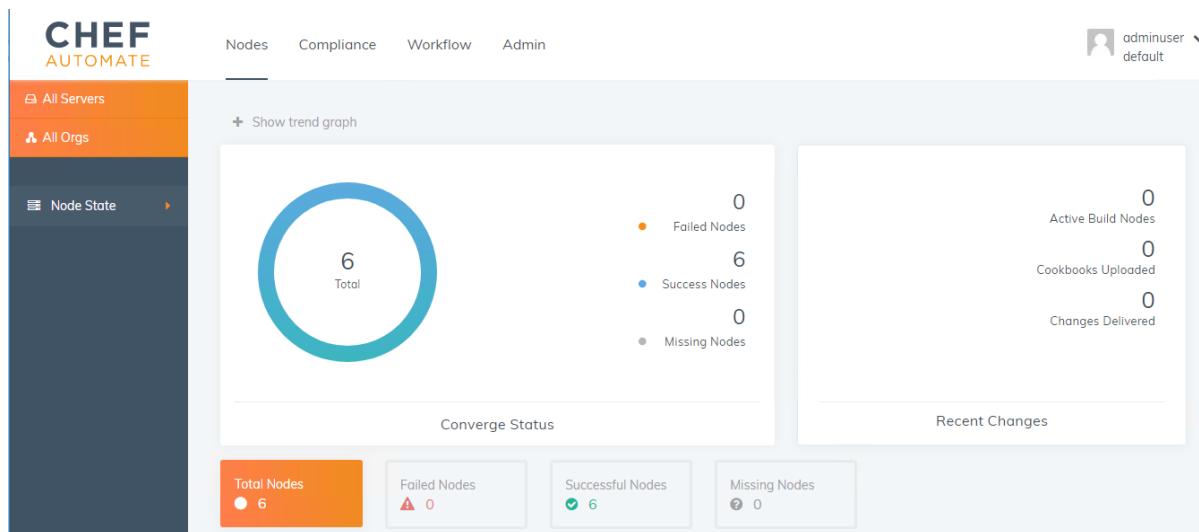
1. Using **workstationFQDN**, Login to the ChefWorkStation with **adminUsername** provided in the outputs section and password as **adminPassword** used during template deployment.

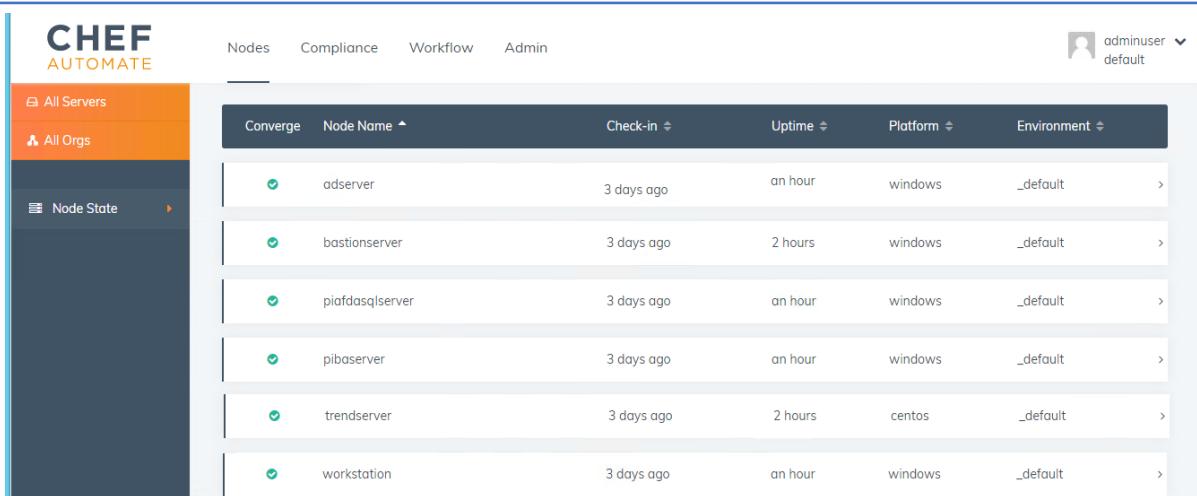


2. Copy and paste the **chefAutomateIPAddress** in a browser which is provided in the outputs section. Login with the **chefAutomateLoginUsername** and **adminPassword** used during template deployment.



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

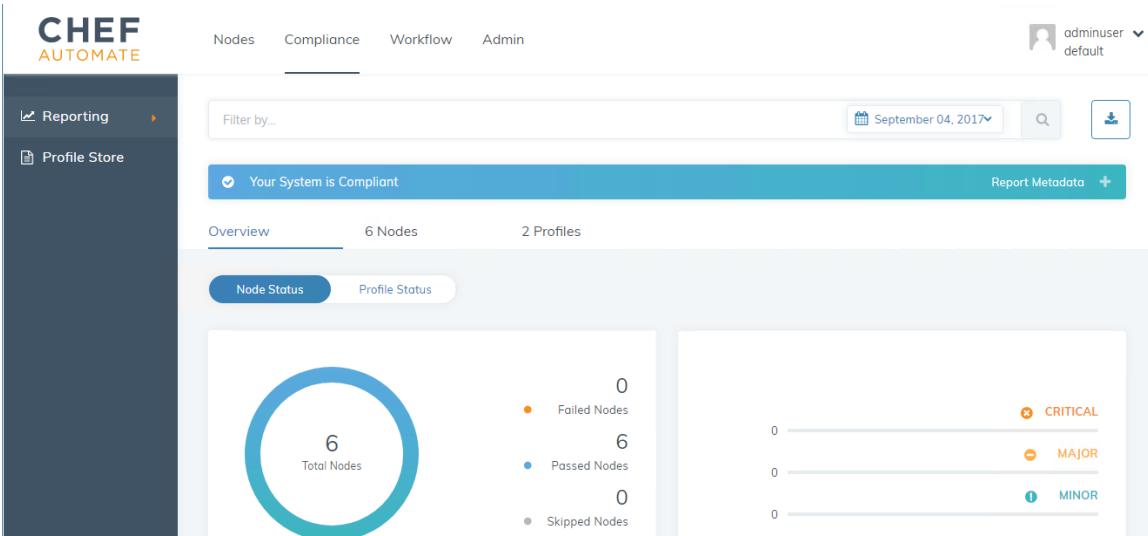




Converge	Node Name	Check-in	Uptime	Platform	Environment
✓	adserver	3 days ago	an hour	windows	_default
✓	bastionserver	3 days ago	2 hours	windows	_default
✓	piafdasqlserver	3 days ago	an hour	windows	_default
✓	pibaserver	3 days ago	an hour	windows	_default
✓	trendserver	3 days ago	2 hours	centos	_default
✓	workstation	3 days ago	an hour	windows	_default

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.



Your System is Compliant

Overview 6 Nodes 2 Profiles

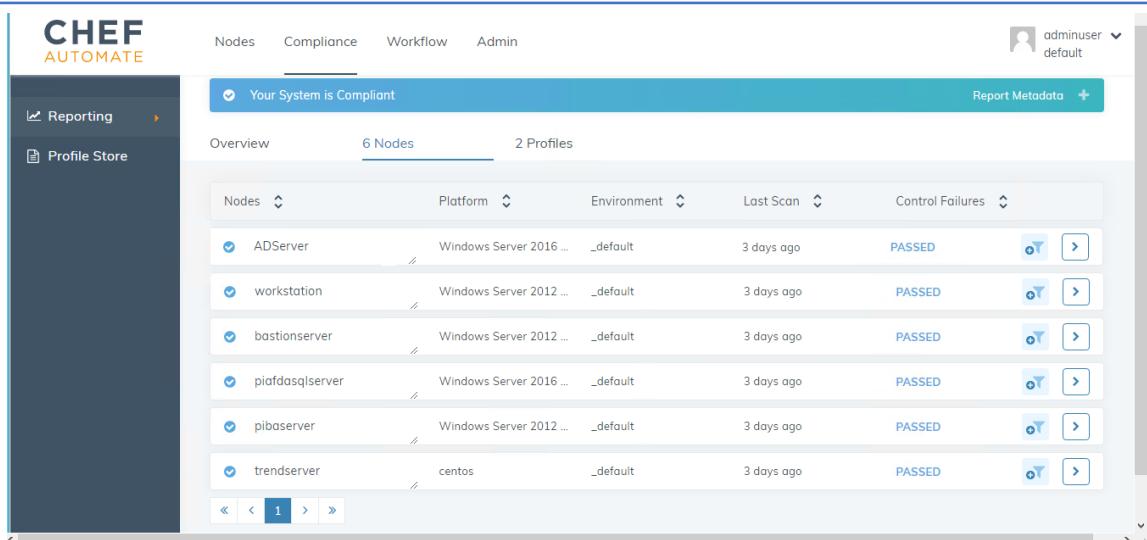
Node Status Profile Status

6 Total Nodes

0 Failed Nodes
6 Passed Nodes
0 Skipped Nodes

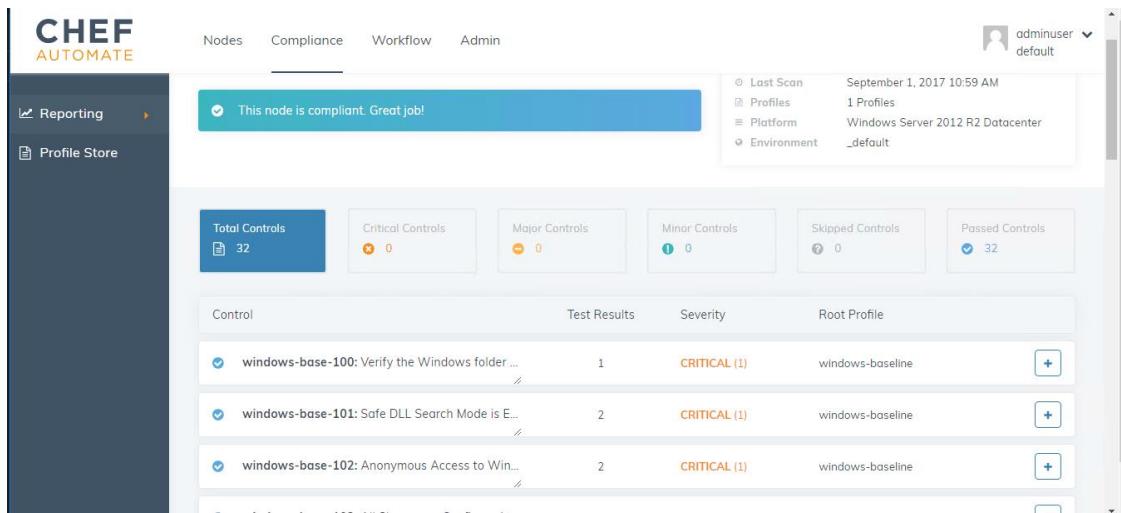
0 Critical
0 Major
0 Minor

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



The screenshot shows the CHEF AUTOMATE web interface under the 'Compliance' tab. A prominent message at the top says 'Your System is Compliant'. Below this, there's an 'Overview' section with tabs for 'Nodes' (selected), 'Platform', 'Environment', 'Last Scan', and 'Control Failures'. The 'Nodes' table lists six nodes: ADServer, workstation, bastionserver, piafdasqlserver, pibaserver, and trendserver. Each node entry includes its name, platform (Windows Server 2016 or centos), environment (_default), last scan (3 days ago), and status (PASSED). To the right of each node entry are two small blue icons.

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



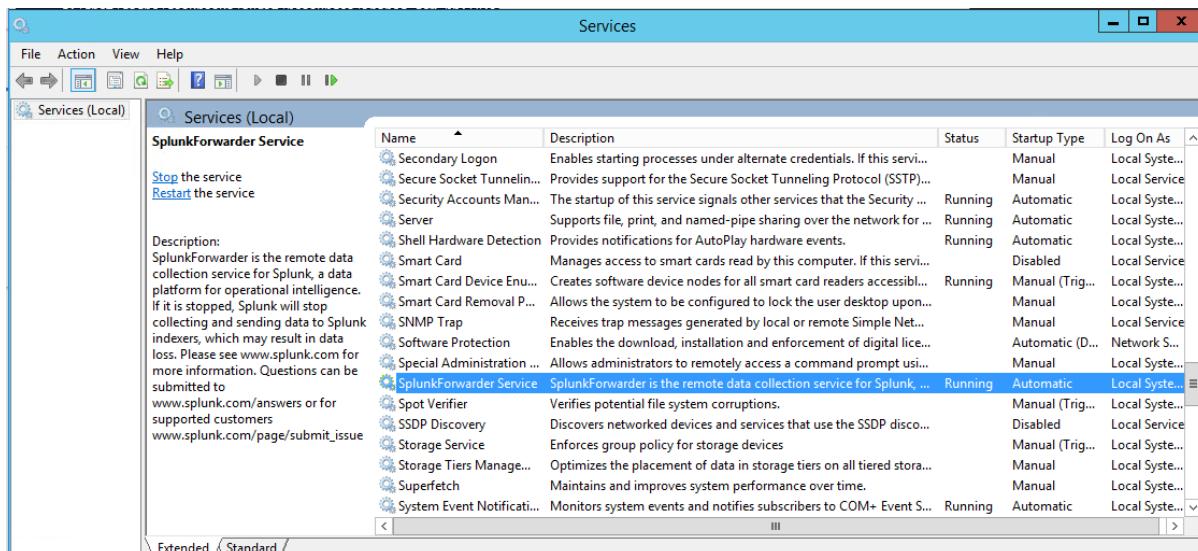
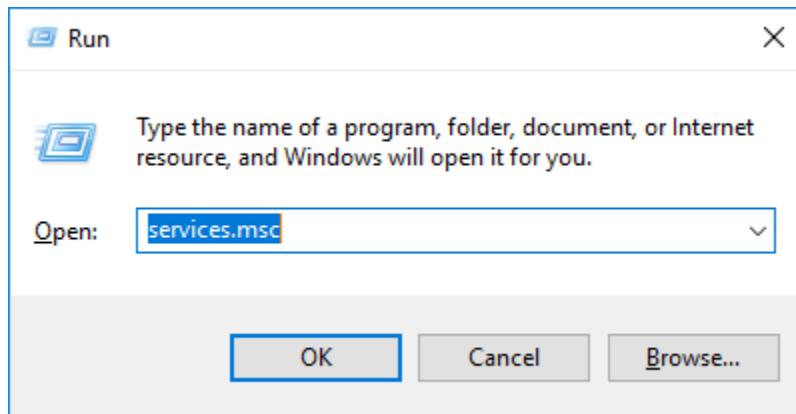
This screenshot shows the same interface as above, but for a specific node named 'workstation'. A message at the top says 'This node is compliant. Great job!'. Below it, a summary box provides details about the last scan (September 1, 2017 10:59 AM), profiles (1 Profiles), platform (Windows Server 2012 R2 Datacenter), and environment (_default). The main area displays a table of controls. The columns are 'Control', 'Test Results', 'Severity', and 'Root Profile'. Three rows are shown, all of which are CRITICAL (1) and belong to the 'windows-baseline' profile. Each row has a '+' icon to its right.

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.



The screenshot shows the Splunk Enterprise search interface. On the left, there's a sidebar with a green header labeled 'Search & Reporting'. Below it is a large dashed box placeholder. The main content area has a title 'Explore Splunk Enterprise' and four circular icons with text below them:

- Product Tours**: An icon of two arrows pointing right and left. Description: 'New to Splunk? Take a tour to help you on your way.'
- Add Data**: An icon of a cylinder with a downward arrow. Description: 'Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.'
- Explore Data**: An icon of a cylinder with horizontal lines. Description: 'Explore data and define how Hunk parses that data.'
- Splunk Apps**: An icon of a box with a gear inside. Description: 'Apps and add-ons extend the capabilities of Splunk Enterprise.'

At the bottom right of the main content area is a 'Close' button.

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

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with links for 'Search & Reporting', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a green header bar with tabs for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area has a search bar with placeholder text 'enter search here...' and a date range selector 'Last 24 hours' with a search icon. A link 'No Event Sampling' is visible. On the right, there's a 'Smart Mode' toggle. The central part of the page is divided into two columns. The left column, titled 'How to Search', contains a paragraph about search features and links to 'Documentation' and 'Tutorial'. The right column, titled 'What to Search', displays event statistics: 585,582 Events INDEXED, a month ago EARLIEST EVENT, and a few seconds ago LATEST EVENT. There's also a 'Data Summary' button. At the bottom, there's a 'Search History' section with a link to expand it.



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

The screenshot shows the Splunk search interface. At the top, there's a navigation bar with links for Administrator, Messages, Settings, Activity, Help, and Find. Below the navigation bar is a search bar containing the query "host='bastionserver'". To the right of the search bar are filters for "Last 24 hours" and a search button. The main area has sections for "How to Search" (with links to Documentation and Tutorial) and "What to Search" (showing 129,781 indexed events from a month ago to a few seconds ago). Below these sections is a "Search History" link. The main search results table has columns for Time, Event, and Fields. It shows two events related to the host 'bastionServer'. The first event is from 08/30/2017 at 12:21:25 PM, and the second is from 08/30/2017 at 12:21:04 PM. Both events are from the LogName=Security source and have EventCode=4625 and EventType=0. The interface also includes a timeline, zoom controls, and a page navigation bar at the bottom.

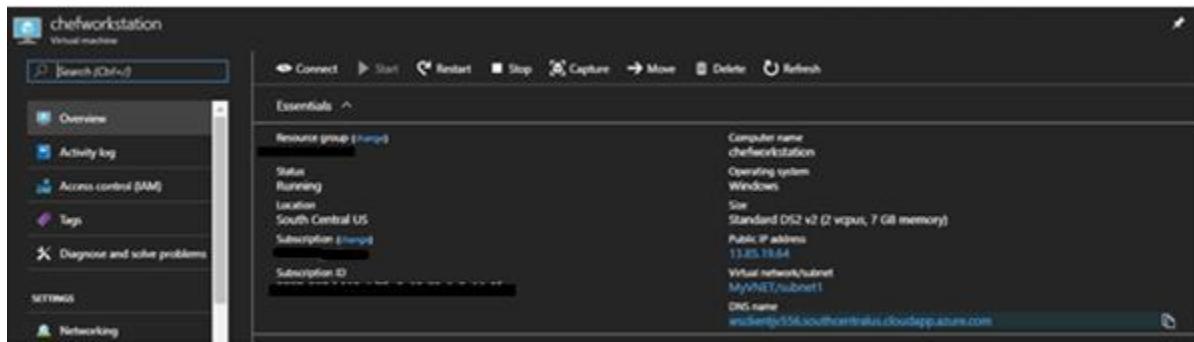
Time	Event
08/30/2017 12:21:25 PM	LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Show all 61 lines host = bastionServer source = WinEventLog.Security sourcetype = WinEventLog.Security
08/30/2017 12:21:04 PM	LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Show all 61 lines host = bastionServer source = WinEventLog.Security sourcetype = WinEventLog.Security

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

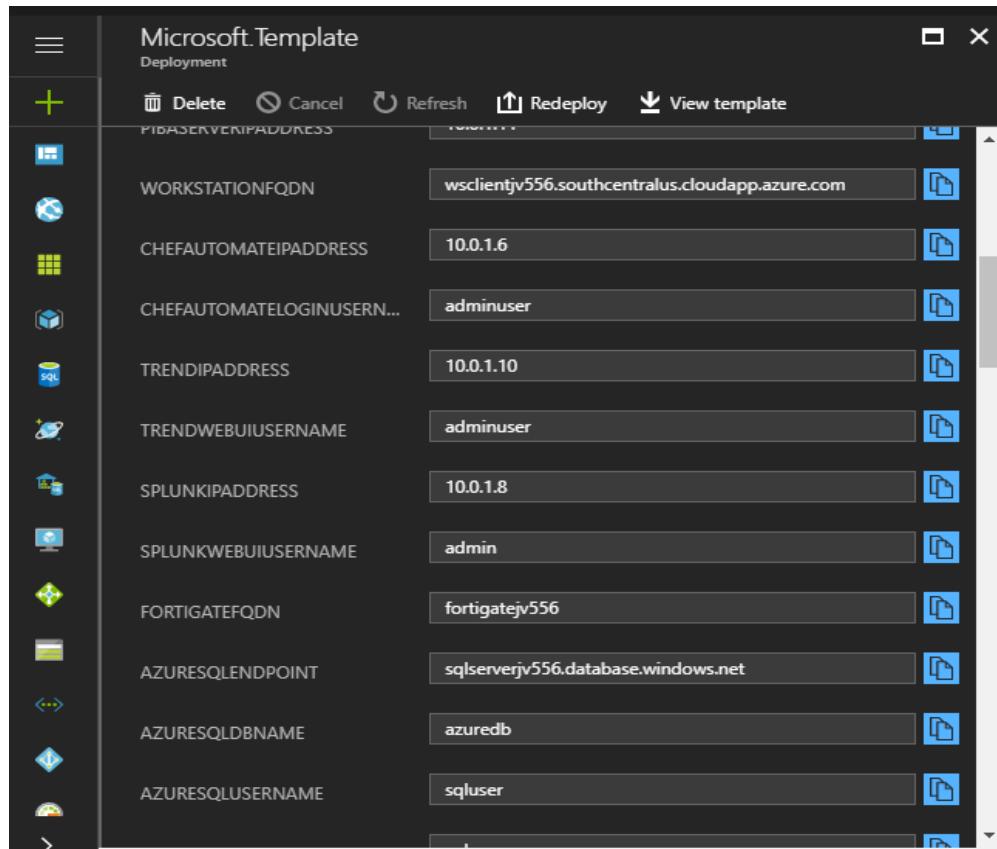
7.4. TrendMicro

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

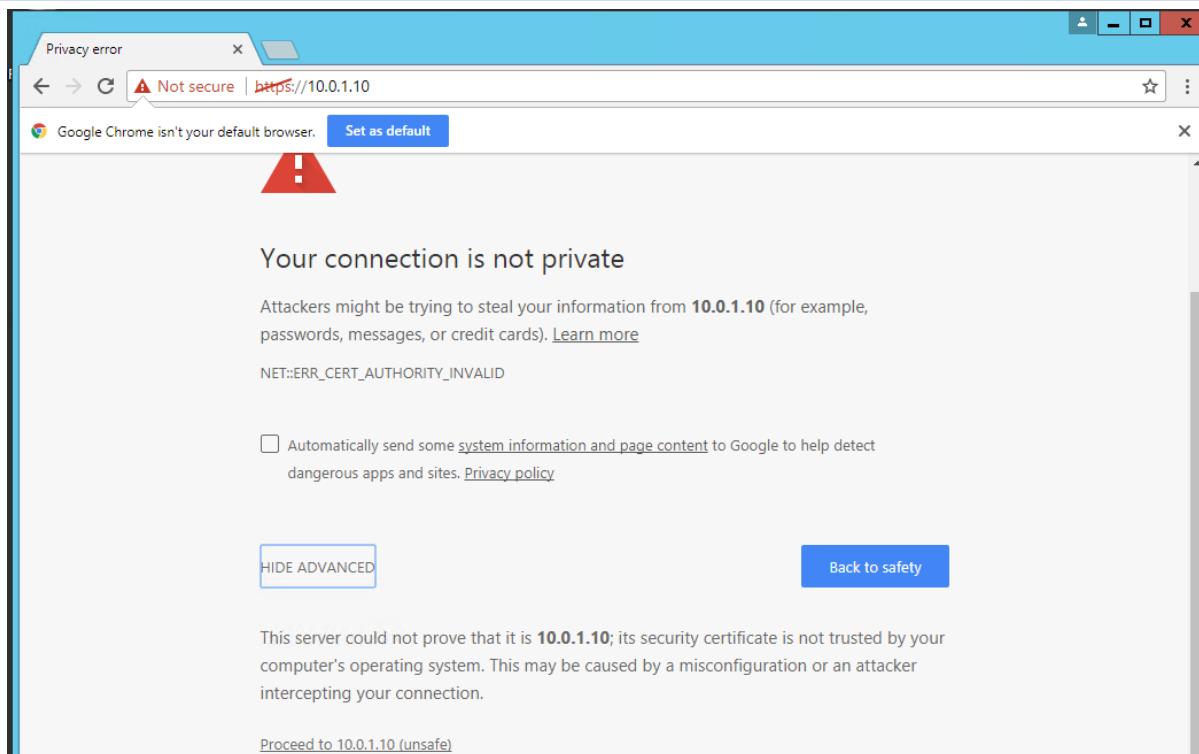
Login to Bastion Host or ChefWorkstation server.



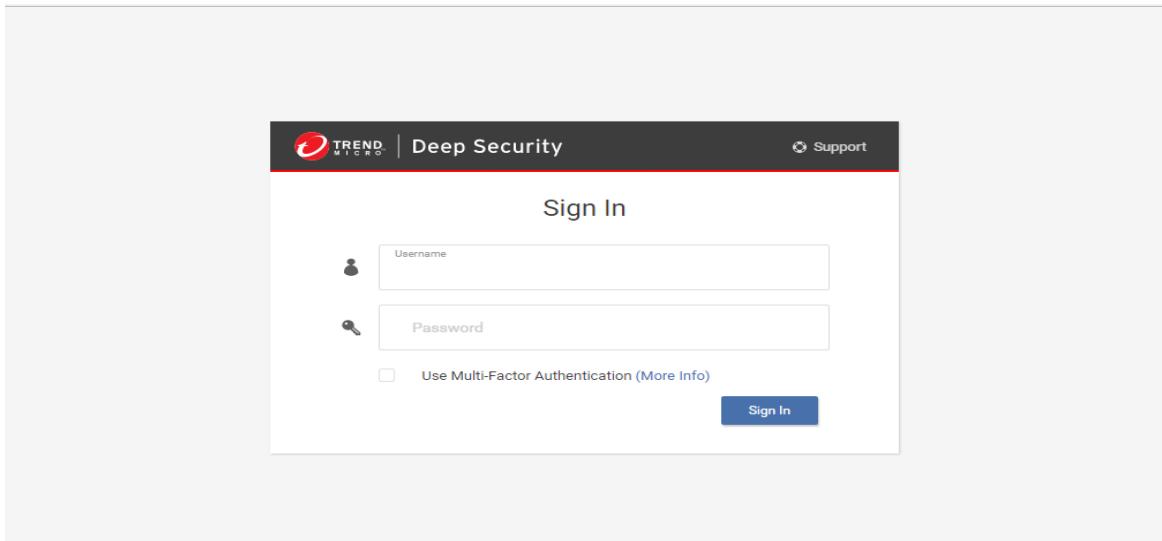
Once login open Browser and enter the TrendMicro IP address, which we get from output section of IOT ARM Template.



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.

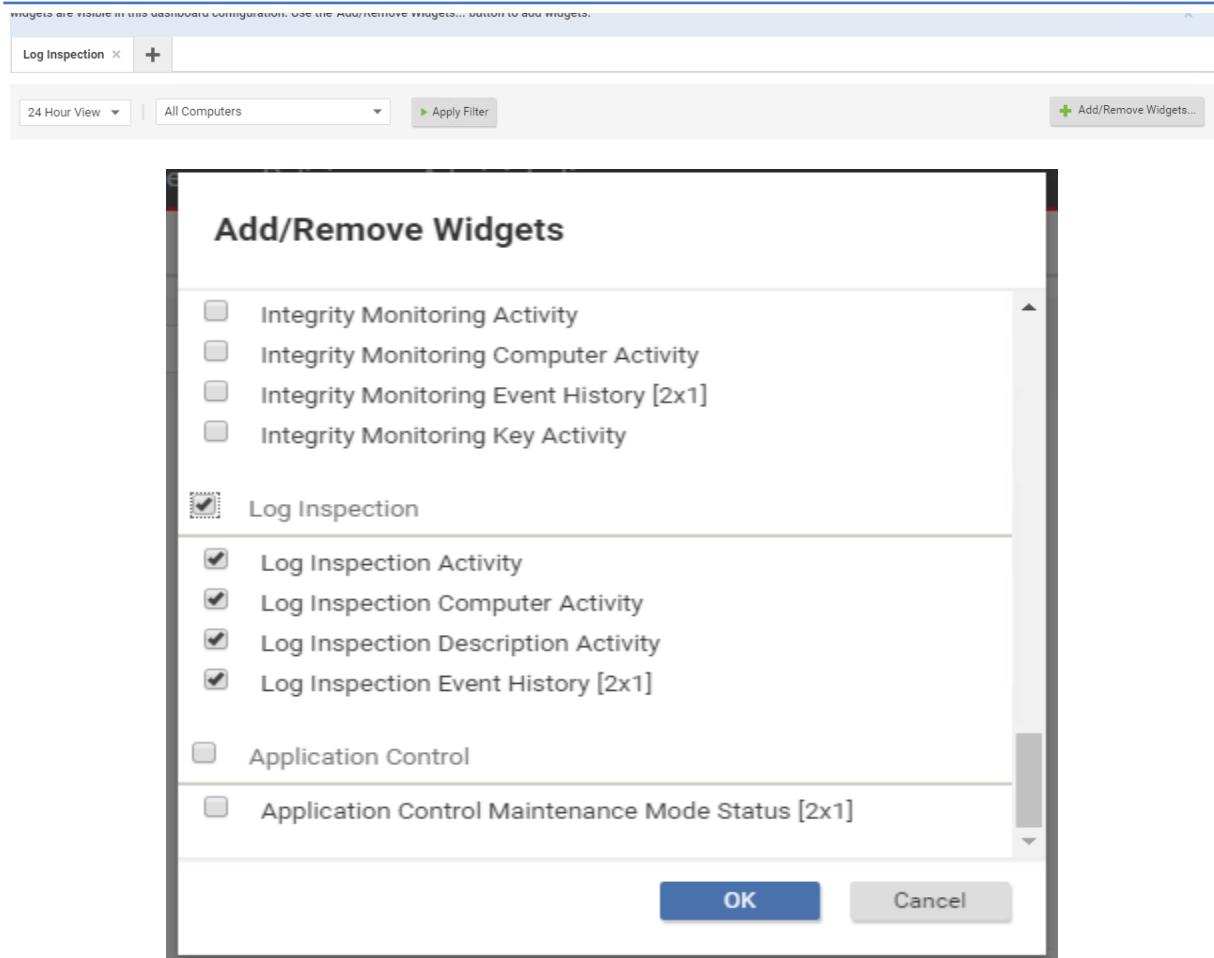
The screenshot shows the Trend Micro Deep Security dashboard. At the top, there's a header with the Trend Micro logo, 'Deep Security', user info ('adminuser'), and a search bar. Below the header is a navigation bar with tabs: Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, and Administration. The 'Dashboard' tab is selected. Under the navigation bar, there's a toolbar with buttons for 'Default' and '+'. The main area contains several widgets:

- Alert Status:** Shows 0 Critical and 7 Warning alerts. A list of latest alerts is provided, all of which are Cloud Computer Not Managed and are 4 hours old.
- Computer Status:** Displays a large green circle indicating 100% managed status. Below it, a table shows the status distribution: Critical (0), Warning (0), Managed (8), and Unmanaged (0).
- My User Summary:** Shows details for the user 'adminuser': ROLE (Full Access), LAST SIGN-IN (August 31, 2017 12:28), and PREVIOUS SIGN-IN (N/A).
- Ransomware Status:** Shows 0 ransomware events.
- Ransomware Event History:** Shows 0 events.

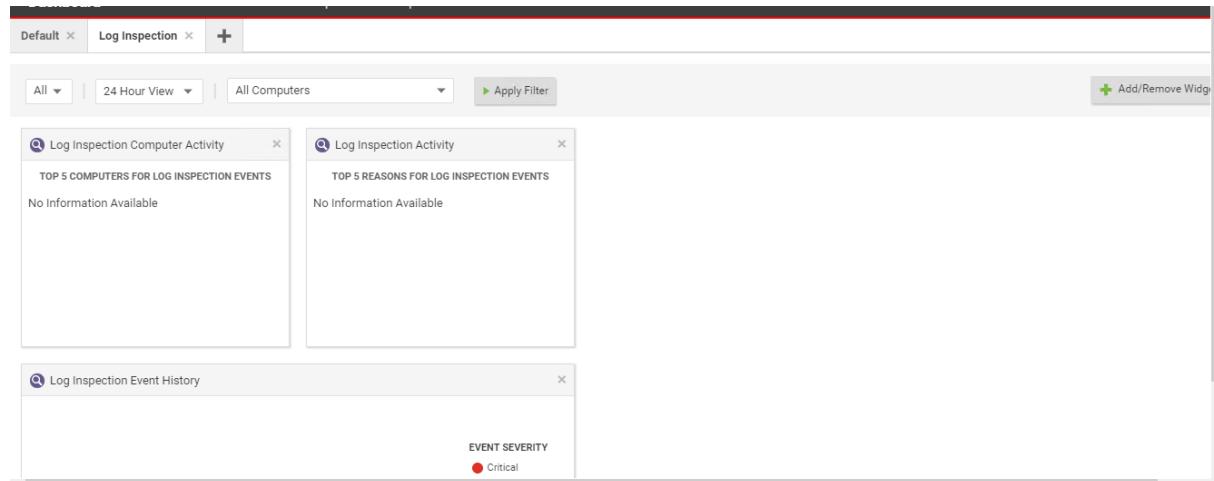
We can create our own Dashboard by clicking on "+" icon Besides Default and add the Widgets which you want to monitor.

The screenshot shows the 'Add New Dashboard' dialog box. It has a title 'Add New Dashboard' and a 'New Dashboard Name:' field containing 'Log Inspection'. There's also a checked checkbox for 'Duplicate Current Dashboard'. At the bottom are 'Add' and 'Cancel' buttons.

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.



The screenshot shows the Trend Micro Deep Security interface. The top navigation bar includes links for Dashboard, Actions, Alerts, Events & Reports, Computers (highlighted in red), Policies, and Administration. The user is logged in as 'adminuser'. The main content area displays a list of computers under the 'Computers' tab. The table has columns for NAME, DESCRIPTION, PLATFORM, POLICY, STATUS, and MAINTENANCE. The status column uses green dots to indicate managed status. The table shows 8 entries, all of which are managed and online.

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENANCE
10.0.0.5	Microsoft Win...	None	Managed (Online)	N/A	
10.0.0.6	Microsoft Win...	None	Managed (Online)	N/A	
10.0.1.10	Red Hat Enter...	Deep Security ...	Managed (Online)	N/A	
10.0.1.11	Microsoft Win...	None	Managed (Online)	N/A	
10.0.1.4	Microsoft Win...	None	Managed (Online)	N/A	
10.0.1.5	Microsoft Win...	None	Managed (Online)	N/A	
10.0.1.6	Ubuntu Linux ...	None	Managed (Online)	N/A	
10.0.1.8	Ubuntu Linux ...	None	Managed (Online)	N/A	

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

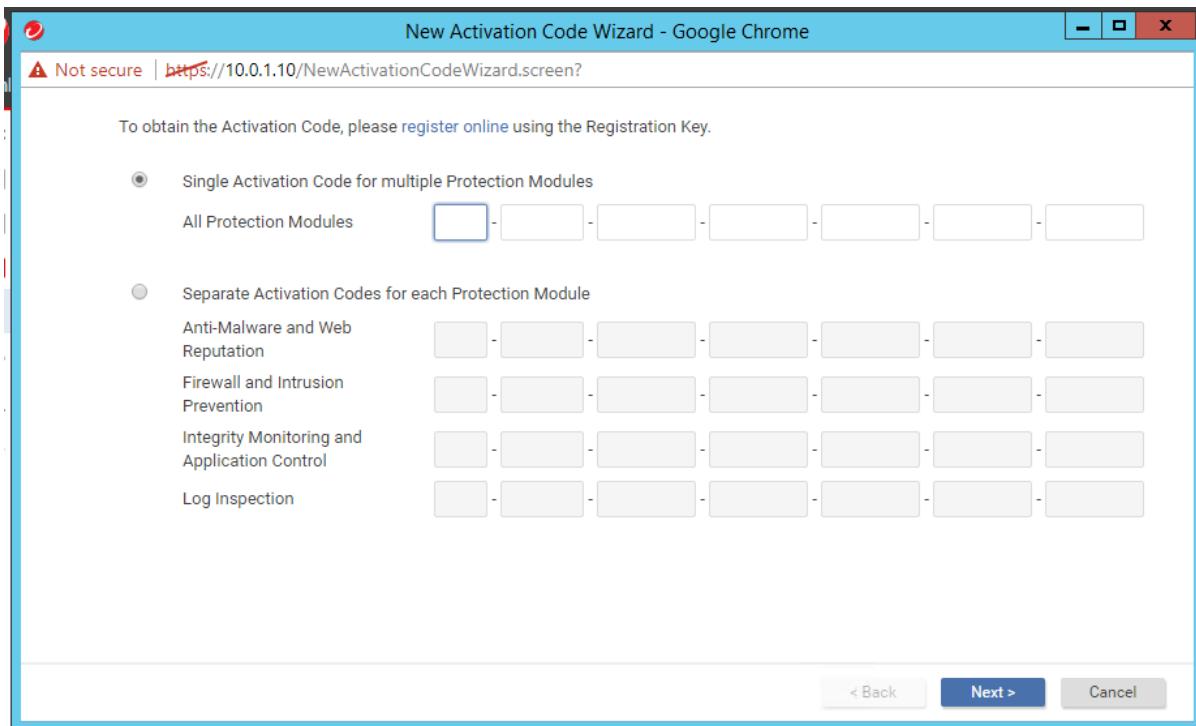
Click on **Licenses** from left side menu and then Click on **Enter New Activation Code**

The screenshot shows the Trend Micro Deep Security interface with the 'Administration' tab selected. The left sidebar has a 'Licenses' section highlighted. The main content area shows a table of licensed modules. The table has columns for Status, Type, and Expires. All modules listed are currently not licensed. A button at the bottom allows entering a new activation code.

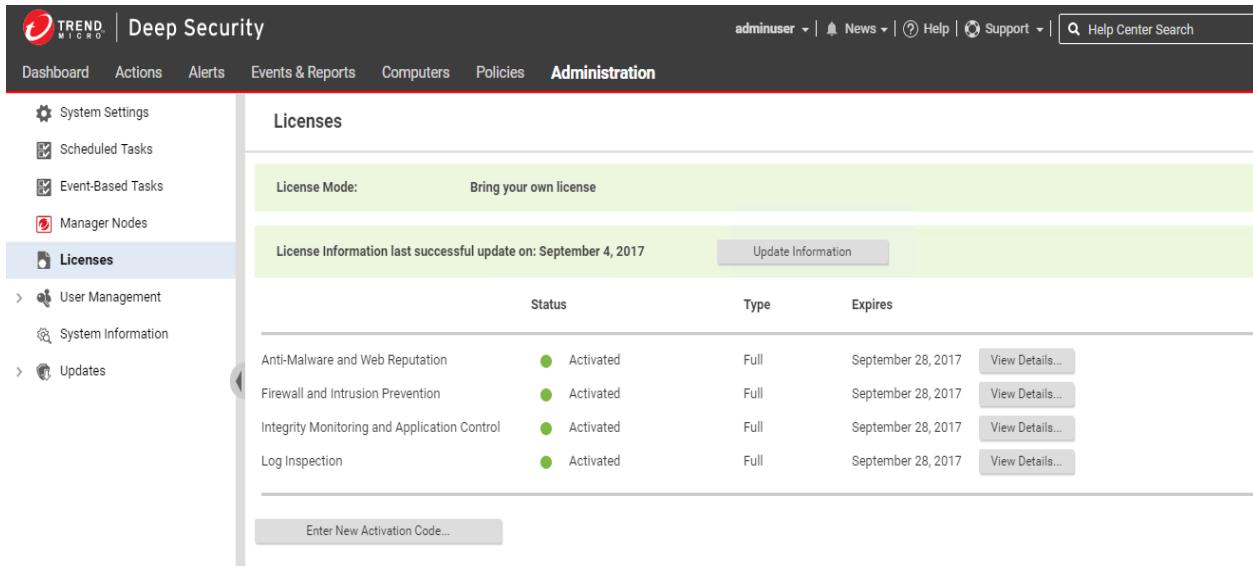
	Status	Type	Expires	
Anti-Malware and Web Reputation	Not Licensed	N/A	N/A	View Details...
Firewall and Intrusion Prevention	Not Licensed	N/A	N/A	View Details...
Integrity Monitoring and Application Control	Not Licensed	N/A	N/A	View Details...
Log Inspection	Not Licensed	N/A	N/A	View Details...

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**.



	Status	Type	Expires
Anti-Malware and Web Reputation	Activated	Full	September 28, 2017
Firewall and Intrusion Prevention	Activated	Full	September 28, 2017
Integrity Monitoring and Application Control	Activated	Full	September 28, 2017
Log Inspection	Activated	Full	September 28, 2017

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**

TREND MICRO | Deep Security

adminuser | News | Help | Support | Help Center Search

Dashboard Actions Alerts Events & Reports Computers Policies Administration

Smart Folders Computers

Computers With sub-Groups By Group

Add Delete Details Actions Events Export Columns

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENAN...	SEND POLICY SUCESSFUL
Computers (8)						
10.0.0.5	Microsoft Win...	None	Managed (Online)	N/A	11 Minutes Ago	
10.0.0.6	Microsoft Win...	None	Managed (Online)	N/A	August 31, 2017 13:47	
10.0.1.10	Red Hat Enter...	Deep Security ...	Managed (Online)	N/A	September 2, 2017 07:30	
10.0.1.11	Microsoft Win...	None	Managed (Online)	N/A	August 31, 2017 13:43	
10.0.1.4	Microsoft Win...	None	Managed (Online)	N/A	August 31, 2017 13:42	
10.0.1.5	Microsoft Win...	None	Managed (Online)	N/A	4 Minutes Ago	
10.0.1.6	Ubuntu Linux ...	None	Managed (Online)	N/A	August 31, 2017 13:41	
10.0.1.8	Ubuntu Linux ...	None	Managed (Online)	N/A	August 31, 2017 13:39	

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

Click on Anti-Malware from left side menu.

Computer: 10.0.0.6

General Actions System Events

Hostname: 10.0.0.6 (Last IP Used: 10.0.0.6)

Display Name:

Description:

Platform: Microsoft Windows Server 2012 R2 (64 bit) Build 9600

Group: Computers

Policy: None

Asset Importance: None

Download Security Updates From: Default Relay Group

Agent

- Managed (Online)
- Off, not installed, no configuration
- Off, not installed
- Off, not installed, no rules
- Off, not installed, no rules
- Off, not installed, no rules
- Off, not supported

Yes

Save Close

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.

Computer: 10.0.0.6

General	Smart Protection	Advanced	Identified Files	Anti-Malware Events
Anti-Malware				
Configuration: Default (Off)				
State: Off, not installed, no configuration				
Real-Time Scan				
<input checked="" type="checkbox"/> Inherited				
Malware Scan Configuration: No Configuration	<input type="button" value="Edit"/>			
Schedule: Select Schedule	<input type="button" value="Edit"/>			
Manual Scan				
<input checked="" type="checkbox"/> Inherited				
Malware Scan Configuration: No Configuration	<input type="button" value="Edit"/>			
Scheduled Scan				
<input checked="" type="checkbox"/> Inherited				
Malware Scan Configuration: No Configuration	<input type="button" value="Edit"/>			
Malware scan				
Last Manual Scan for Malware: N/A				
<input type="button" value="Save"/> <input type="button" value="Close"/>				

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

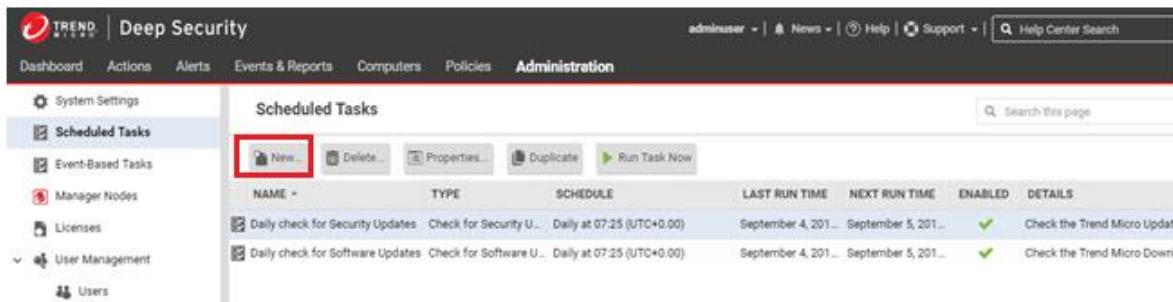
Note: it might take some time to get Activated.

Computer: 10.0.0.6

General	Actions	System Events
Anti-Malware		
Hostname: 10.0.0.6 (Last IP Used: 10.0.0.6)		
Display Name:		
Description:		
Platform: Microsoft Windows Server 2012 R2 (64 bit) Build 9600		
Group: Computers		
Policy: None	<input type="button" value="Edit"/>	
Asset Importance: None	<input type="button" value="Edit"/>	
Download Security Updates From: Default Relay Group	<input type="button" value="Edit"/>	
Agent		
Task(s)		
<input checked="" type="checkbox"/> Anti-Malware	Managed (Online)	Update of Configuration Pending (Heartbeat)
<input checked="" type="checkbox"/> Web Reputation	On, Real Time	
<input checked="" type="checkbox"/> Firewall	Off, installation pending	
<input checked="" type="checkbox"/> Intrusion Prevention	Off, not installed, no rules	
<input checked="" type="checkbox"/> Integrity Monitoring	Off, not installed, no rules	
<input checked="" type="checkbox"/> Log Inspection	Off, not installed, no rules	
<input checked="" type="checkbox"/> Application Control	Off, not installed, no rules	
Overrides		

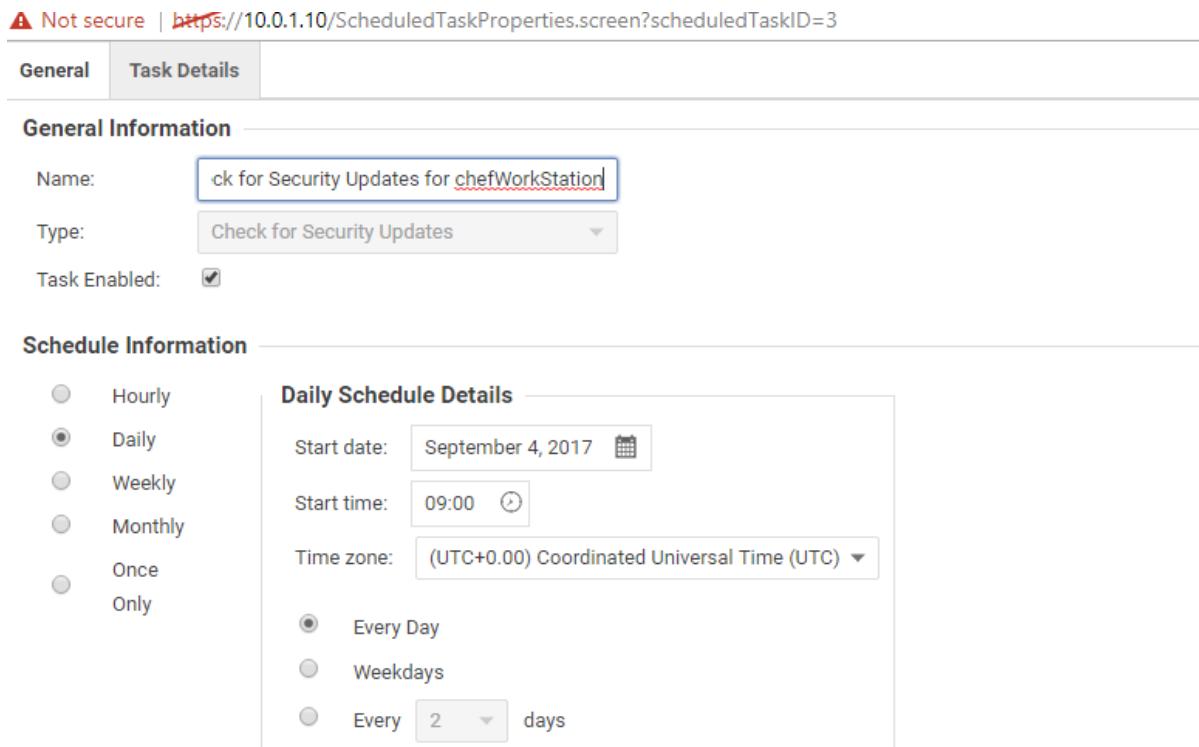
We can schedule a scan for Hourly, Daily, Weekly, Monthly, Only once.

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



The screenshot shows the Trend Micro Deep Security administration interface. The top navigation bar includes links for Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, and Administration. The Administration menu is open, showing options like System Settings, Scheduled Tasks (which is selected and highlighted in blue), Event-Based Tasks, Manager Nodes, Licenses, and User Management. On the right, the 'Scheduled Tasks' section displays a table of tasks. The first task is 'Daily check for Security Updates' and the second is 'Daily check for Software Updates'. Both tasks are set to run daily at 07:25 UTC+0.00. The 'Enabled' column shows green checkmarks, and the 'Details' column indicates they check for updates from Trend Micro.

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



General **Task Details**

General Information

Name: Check for Security Updates for chefWorkStation

Type: Check for Security Updates

Task Enabled:

Schedule Information

Frequency:

- Hourly
- Daily
- Weekly
- Monthly
- Once
- Only

Daily Schedule Details

Start date: September 4, 2017

Start time: 09:00

Time zone: (UTC+0.00) Coordinated Universal Time (UTC)

Frequency:

- Every Day
- Weekdays
- Every days

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

New Scheduled Task Wizard - Google Chrome

A Not secure | <https://10.0.1.10/ScheduledTaskWizard.screen>

Select the computer(s) to update.

All Computers

In Group: Include sub-Groups

Using Policy: Include sub-Policies

Computer:

< Back **Next >**

Enter a unique name for this scheduled task.

Name:

Type: Check for Security Updates

Schedule: Daily at 10:10 (UTC+0:00)

Next Run: September 4, 2017 10:10

Details: Computer: 10.0.0.6

Task Enabled

Run Task on 'Finish'

< Back **Finish** Cancel

Click on Finish

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



Deep Security

Dashboard Actions Alerts Events & Reports Computers Policies Administration

Scheduled Tasks

New... Delete... Properties... Duplicate Run Task Now

NAME	TYPE	SCHEDULE	LAST RUN TIME	NEXT RUN TIME
Daily Check for Security Updates for chefWorkStation	Check for Security U...	Daily at 09:00 (UTC+0:00)	September 4, 201...	September 4, 201...
Daily check for Security Updates	Check for Security U...	Daily at 07:25 (UTC+0:00)	September 4, 201...	September 5, 201...
Daily check for Software Updates	Check for Software U...	Daily at 07:25 (UTC+0:00)	September 4, 201...	September 5, 201...

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

Deep Security

Dashboard Actions Alerts Events & Reports Computers Policies Administration

✓ Running Task: Daily Check for Security Updates for chefWorkStation

Scheduled Tasks

New... Delete... Properties... Duplicate Run Task Now

NAME	TYPE	SCHEDULE	LAST RUN TIME	NEXT RUN TIME
Daily Check for Security Updates for chefWorkStation	Check for Security U...	Daily at 08:06 (UTC+0:00)	September 4, 201...	Running

Performing Security Update on 1 Computer

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

Dashboard Actions Alerts Events & Reports Computers Policies Administration

Computers With sub-Groups By Group

Add Delete... Details... Actions... Events... Export... Columns...

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENANCE	SEND POLICY	SUCCESSFUL
Computers (8)							
10.0.0.5		Microsoft Win...	None	Managed (Online)	N/A		2 Hours Ago
10.0.0.6		Microsoft Win...	None	Managed (Online)	N/A		48 Minutes Ago

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

Computer: 10.0.0.6

Overview	General	Actions	System Events																	
<ul style="list-style-type: none"> Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Application Control Interfaces Settings 	<p>System Events All ▾ No Grouping ▾</p> <p>Period: Last Hour</p> <p>Computers: Computer: 10.0.0.6</p> <p>View Export Auto-Tagging... Columns...</p> <table border="1"> <thead> <tr> <th>TIME</th> <th>LEVEL</th> <th>EVENT ID</th> <th>EVENT</th> <th>TAG(S)</th> <th>EVENT ORIGI...</th> </tr> </thead> <tbody> <tr> <td>September 4, 2017 09:03:53</td> <td>Info</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td></td> </tr> <tr> <td>September 4, 2017 09:00:25</td> <td>Info</td> <td>273</td> <td>Security Update: Security Update Check and Download Requested</td> <td>Manager</td> <td></td> </tr> </tbody> </table>	TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...	September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent		September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager		<p>Search this page</p>
TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...															
September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent																
September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager																

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.

Not secure | <https://10.0.1.10/ComputerEditor.screen?hostID=8>

Computer: 10.0.0.6

Overview	General	Actions	System Events																																																											
<ul style="list-style-type: none"> Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Application Control Interfaces Settings Updates Overrides 	<p>System Events All ▾ No Grouping ▾</p> <p>Period: Last Hour</p> <p>Computers: Computer: 10.0.0.6</p> <p>View Export Auto-Tagging... Columns...</p> <table border="1"> <thead> <tr> <th>TIME</th> <th>LEVEL</th> <th>EVENT ID</th> <th>EVENT</th> <th>TAG(S)</th> <th>EVENT ORIGI... TAR</th> </tr> </thead> <tbody> <tr> <td>September 4, 2017 09:03:53</td> <td>Info</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 09:00:25</td> <td>Info</td> <td>273</td> <td>Security Update: Security Update Check and Download Requested</td> <td>Manager</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>Select All (14)</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>Export Selected to CSV...</td> <td>273</td> <td>Security Update: Security Update Check and Download Requested</td> <td>Manager</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>View</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>Events Retrieved</td> <td>710</td> <td></td> <td>Agent</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>Add Tag(s)...</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:59:59</td> <td>Remove Tag(s)...</td> <td>276</td> <td>Update: Summary Information</td> <td>Manager</td> <td>10.0</td> </tr> <tr> <td>September 4, 2017 08:15:40</td> <td>Info</td> <td>2204</td> <td>Security Update: Pattern Update on Agents/Appliances Successful</td> <td>Agent</td> <td>10.0</td> </tr> </tbody> </table>	TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI... TAR	September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0	September 4, 2017 08:59:59	Select All (14)	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	September 4, 2017 08:59:59	Export Selected to CSV...	273	Security Update: Security Update Check and Download Requested	Manager	10.0	September 4, 2017 08:59:59	View	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	September 4, 2017 08:59:59	Events Retrieved	710		Agent	10.0	September 4, 2017 08:59:59	Add Tag(s)...	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	September 4, 2017 08:59:59	Remove Tag(s)...	276	Update: Summary Information	Manager	10.0	September 4, 2017 08:15:40	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	<p>Search this page</p>
TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI... TAR																																																									
September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0																																																									
September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0																																																									
September 4, 2017 08:59:59	Select All (14)	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0																																																									
September 4, 2017 08:59:59	Export Selected to CSV...	273	Security Update: Security Update Check and Download Requested	Manager	10.0																																																									
September 4, 2017 08:59:59	View	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0																																																									
September 4, 2017 08:59:59	Events Retrieved	710		Agent	10.0																																																									
September 4, 2017 08:59:59	Add Tag(s)...	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0																																																									
September 4, 2017 08:59:59	Remove Tag(s)...	276	Update: Summary Information	Manager	10.0																																																									
September 4, 2017 08:15:40	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0																																																									

Overview

- Anti-Malware
- Web Reputation
- Firewall
- Intrusion Prevention
- Integrity Monitoring
- Log Inspection
- Application Control
- Interfaces
- Settings
- Updates
- Overrides

System Events

All ▾ No Grouping ▾

Period: Last Hour

Computers: Computer: 10.0.0.6

View Export Auto-Tagging... Columns...

TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...	TAR
September 4, 2017 09:03:53	Info	273	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 09:00:21	Info	Select All (14)	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:25:44	Info	2204	Export Selected to CSV...	Agent	10.0	
September 4, 2017 08:20:21	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:15:31	Info	273	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:15:31	Info	273	Add Tag(s)...	Agent	10.0	
September 4, 2017 08:15:31	Info	273	Remove Tag(s)...	Agent	10.0	
September 4, 2017 08:15:31	Info	273	Events Retrieved	Agent	10.0	
September 4, 2017 08:15:31	Info	273	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	

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

Trend Event logs

Name	Date modified	Type	Size
System_Events (1)	04-09-2017 14:36	Microsoft Excel C...	1 KB
System_Events	04-09-2017 14:36	Microsoft Excel C...	1 KB

Clipboard Font Alignment Number Styles Cells Editing

A	B	C	D	E	F	G	H	I	J	K	L
1 Time	Level	Event ID	Event	Tag(s)	Event Orig	Target	Action By	Manager	Description		
2 September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0.0.6	System	10.0.1.10		Description Omitted		
3											
4											

Clipboard Font Alignment Number Styles Cells Editing

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1 Time	Level	Event ID	Event	Tag(s)	Event Origin	Target	Action By	Manager	Description				
2 September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0.0.6	System	10.0.1.10	Anti-Malware Component Update succeeded					
3													

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.



Deep Security

Dashboard Actions **Alerts** Events & Reports Computers Policies Administration

Alerts Summary View By Time [Configure Alerts...](#)

Computers: All Computers

Recommendations have been made for 1 Computer(s) 1 Hour Ago

Deep Security Manager has determined that the security configuration of one of your computers should be updated. To see what changes are recommended, open the computer's Editor window and look through the module pages for warnings of unresolved recommendations. In the Assigned Rules area, click Assign/Unassign... to display the list of available Rules and then filter them using the "Show Recommended for Assignment" viewing filter option. (Select "Show Recommended for Unassignment" to display Rules that can safely be unassigned.)

Hide Details

Time: September 4, 2017 06:01
Last Updated: September 4, 2017 06:01
Severity: Warning
Computer(s): 10.0.0.5

[Dismiss Selected](#) | [Dismiss All](#)

Licensing for Anti-Malware and Web Reputation Expires (September 28, 2017) August 31, 2017 12:43

The Protection Module licensing will expire soon. You can remove this alert by changing your license on the Administration > Licenses page.

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

Deep Security

Dashboard Actions **Alerts** Events & Reports Computers Policies Administration

Alerts List View No Grouping [Search this page](#)

Computers: All Computers

Search: Severity Equals Warning

[View](#) [Dismiss](#) [Configure Alerts...](#)

TIME	SEVERITY	ALERT	TARGET	SUBJECT
September 4, 2017 06:01	Warning	Recommendation	10.0.0.5	
August 31, 2017 12:43	Warning	Protection Module Licensing Ex...	Log Inspection	Log Inspection
August 31, 2017 12:43	Warning	Protection Module Licensing Ex...	Integrity Moni...	Integrity Monitoring and Application Con...
August 31, 2017 12:43	Warning	Protection Module Licensing Ex...	Firewall and I...	Firewall and Intrusion Prevention
August 31, 2017 12:43	Warning	Protection Module Licensing Ex...	Anti-Malware ...	Anti-Malware and Web Reputation
August 31, 2017 08:13	Warning	Cloud Computer Not Managed ...	10.0.0.6	
August 31, 2017 08:03	Warning	Cloud Computer Not Managed ...	10.0.1.5	
August 31, 2017 07:55	Warning	Cloud Computer Not Managed ...	10.0.0.5	
August 31, 2017 07:55	Warning	Cloud Computer Not Managed ...	10.0.1.1	
August 31, 2017 07:47	Warning	Cloud Computer Not Managed ...	10.0.1.8	

ALERTS 12 0

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

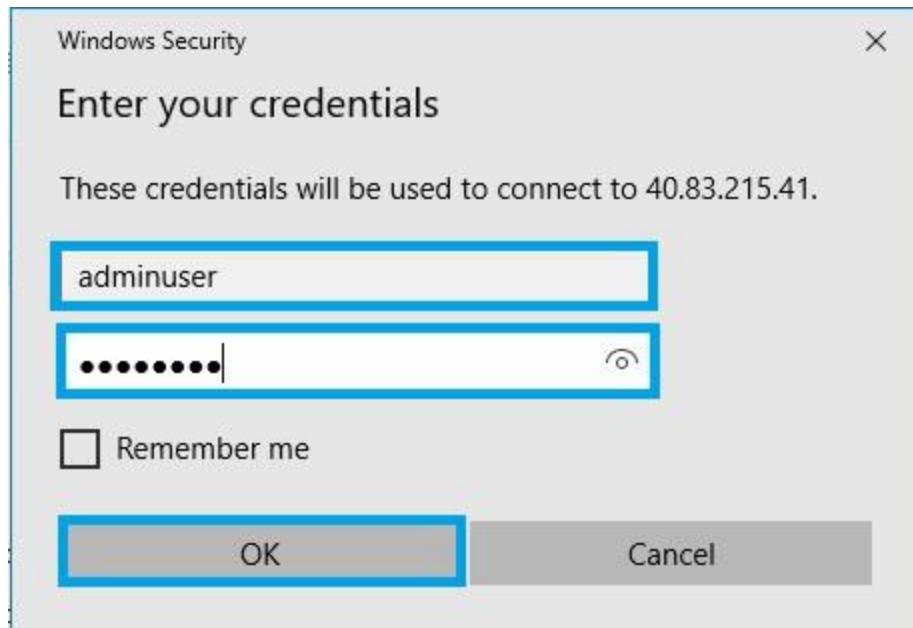
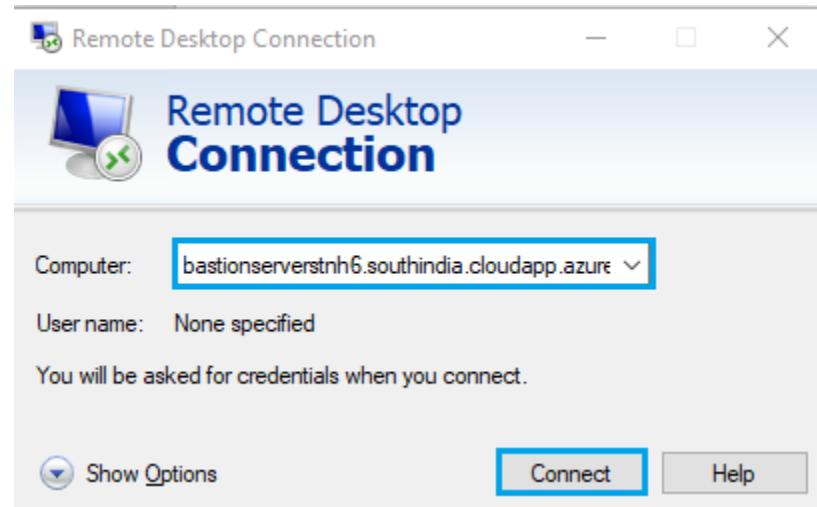
Use the customizable dashboard for quick, at-a-glance, views of the status of your Deep security system. Create scheduled Tasks to periodically send out customizable reports and set up your user account to receive notifications by email of important alerts

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

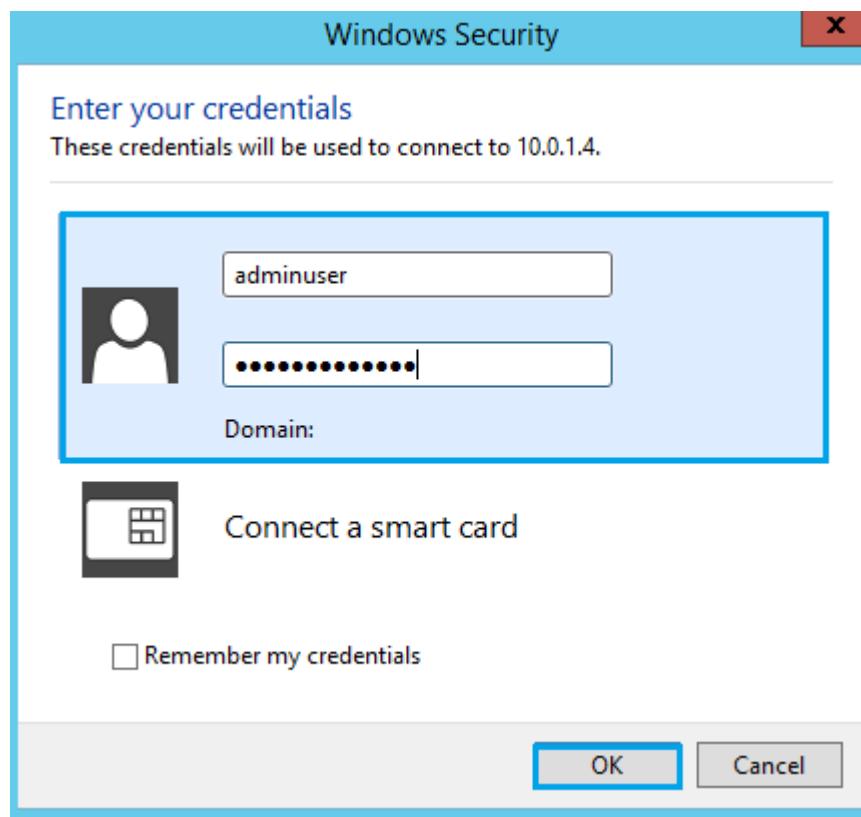
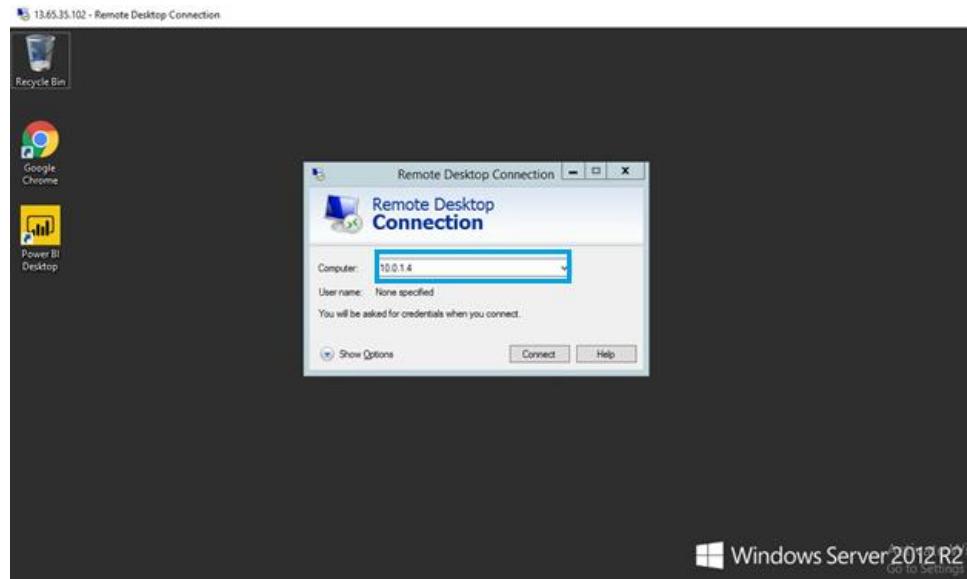
1. Login to the **Bastion Host VM** using **BASTIONFQDN** and **ADMINUSERNAME** provided in the **Outputs** section

Outputs

ADMINUSERNAME	<input type="text" value="adminuser"/>	
BASTIONFQDN	<input type="text" value="bastionserverfevs6.westus.cloudapp.azure.com"/>	
ADSERVERIPADDRESS	<input type="text" value="10.0.1.4"/>	



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

Active Directory Users and Computers

File Action View Help

bastionServer
chefworkstation
PIAFSQLServer
PIBAVMServer

Name	Type
bastionServer	Computer
chefworkstation	Computer
PIAFSQLServer	Computer
PIBAVMServer	Computer

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

File Action View Help

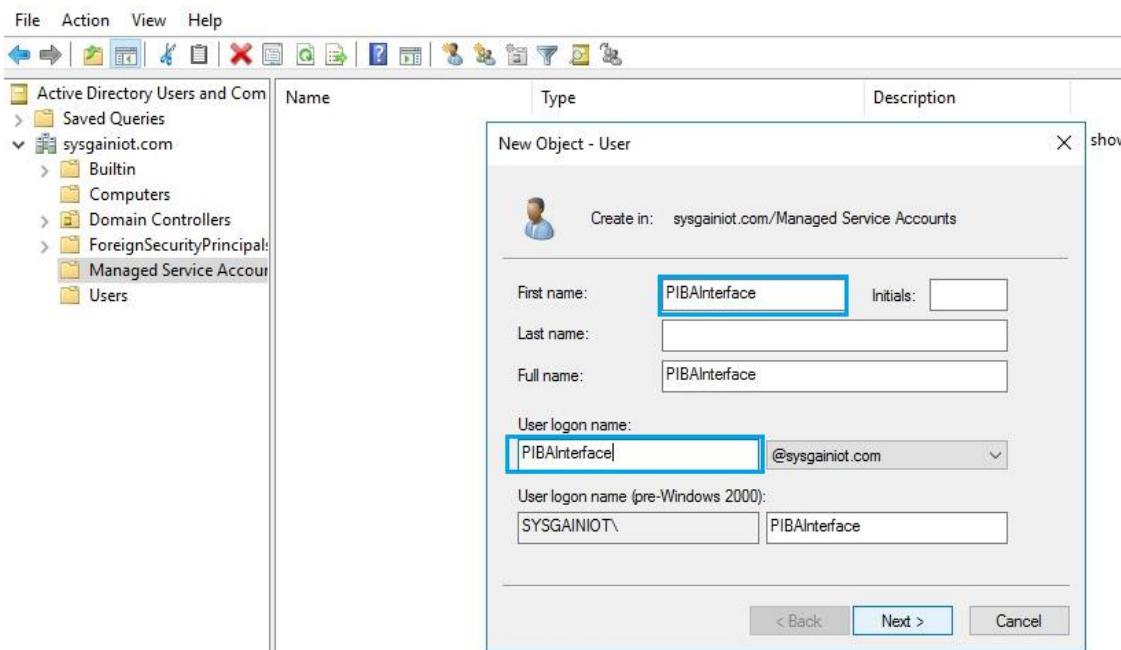
Active Directory Users and Computers

sysgainiot.com

Managed Service Account

New Computer Contact Group InetOrgPerson msDS-KeyCredential msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias Printer User Shared Folder

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 **User must change password at next logon**. Click on **Next**.

New Object - User

Create in: sysgainiot.com/Managed Service Accounts

Password: Confirm password:

User must change password at next logon
 User cannot change password
 Password never expires
 Account is disabled

< Back Next > Cancel

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

Active Directory Users and Computers

File Action View Help

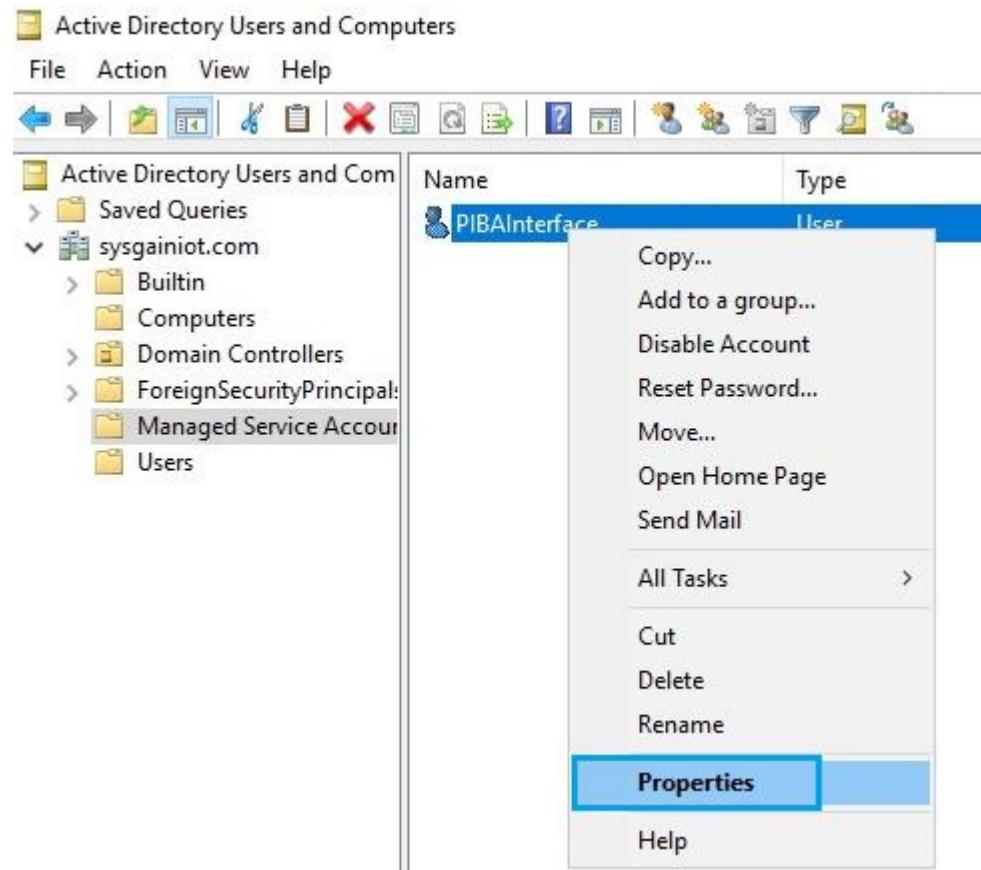
< Back Finish > Cancel

Name	Type	Description
New Object - User	User	sysgainiot.com/Managed Service Accounts

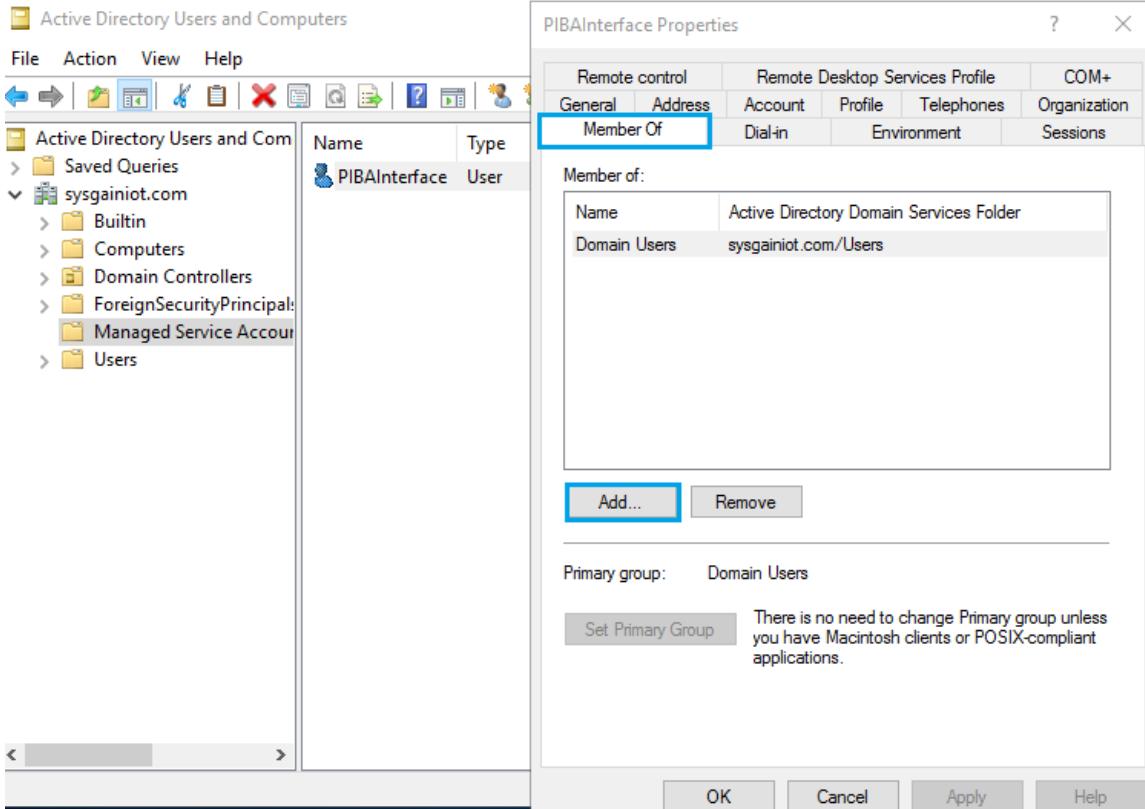
When you click Finish, the following object will be created:

Full name: PIBAInterface
User logon name: PIBAInterface@sysgainiot.com

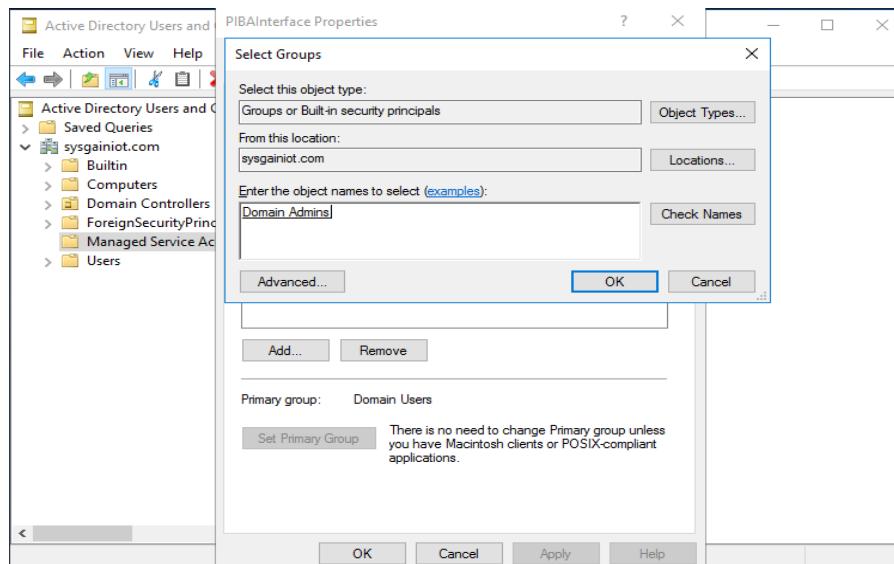
9. Check on the properties of the user created. Right click on the **PIBAInterface** and click on **Properties**.



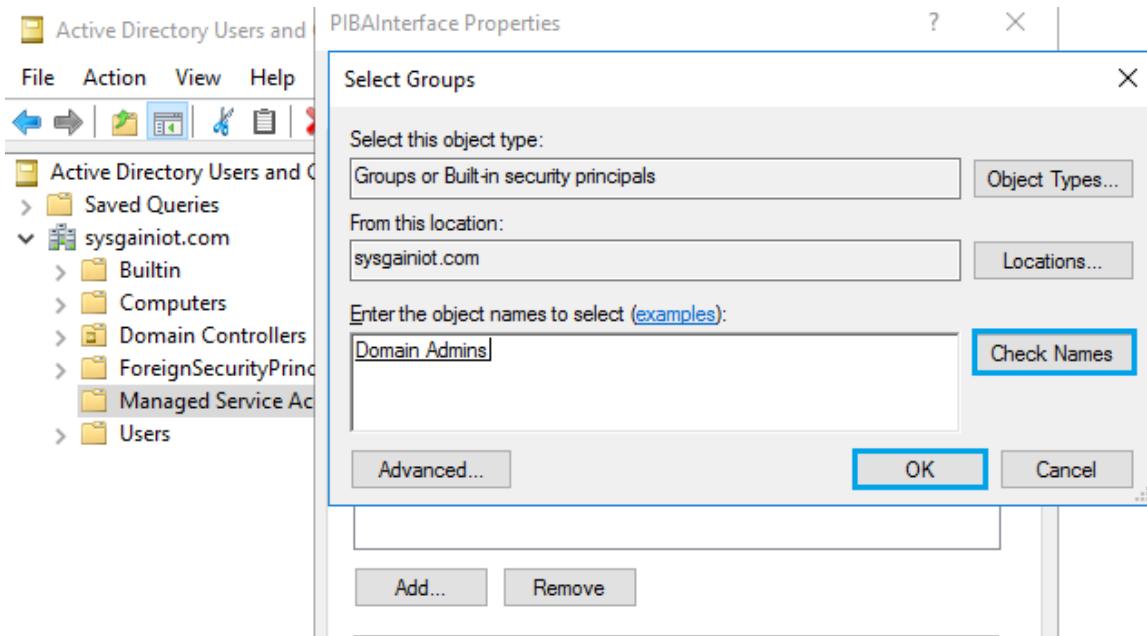
10. A popup will appear. Click on the **Member Of** tab and click the **Add** button.



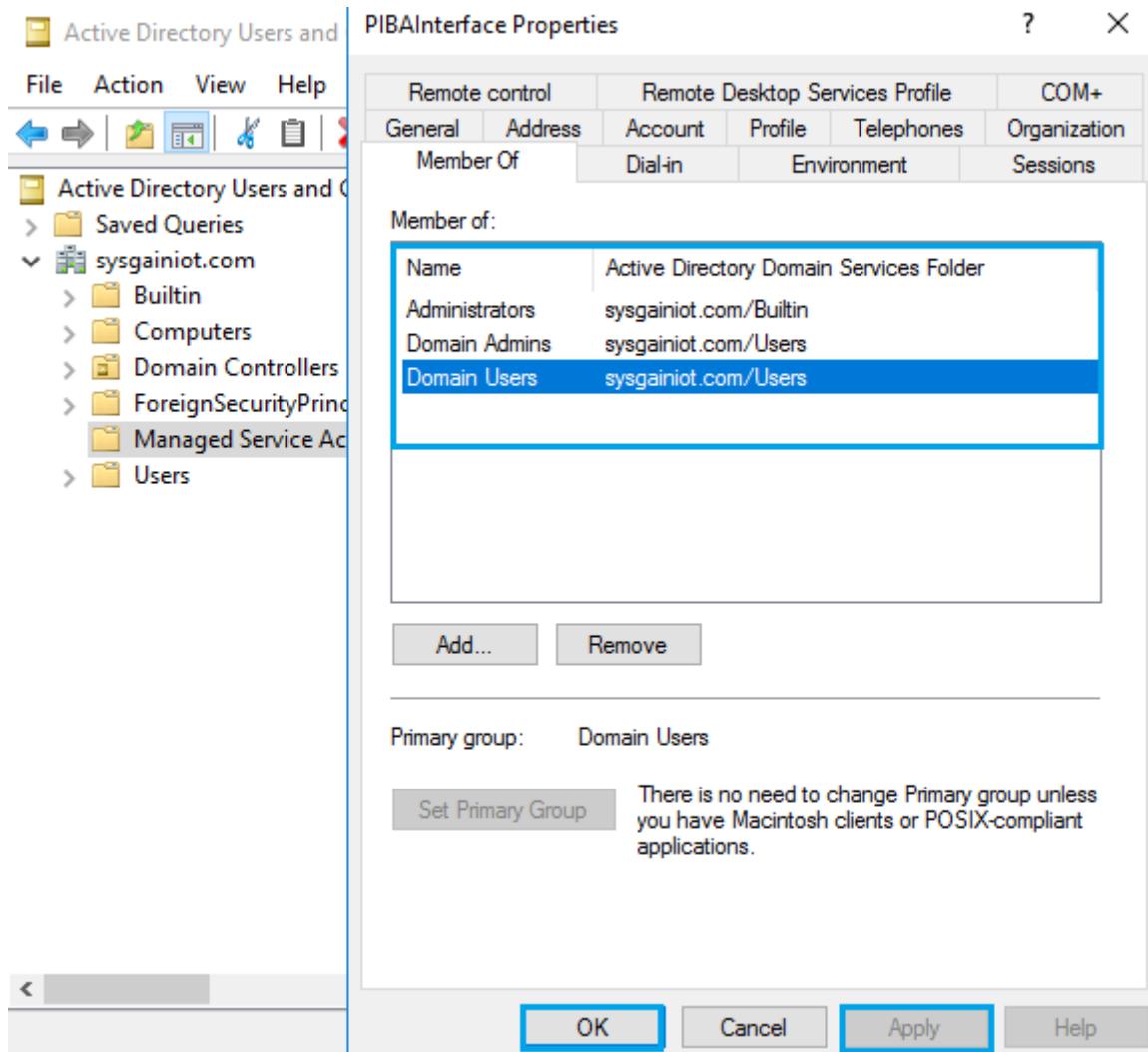
11. Enter the object name as **Domain Admins** and click on **Check Names**. It will display the Domain Admins as object names. Click on **Ok**. After that, click on **Ok** again. You will see the Domain Admin name added to the **Member of** section.



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

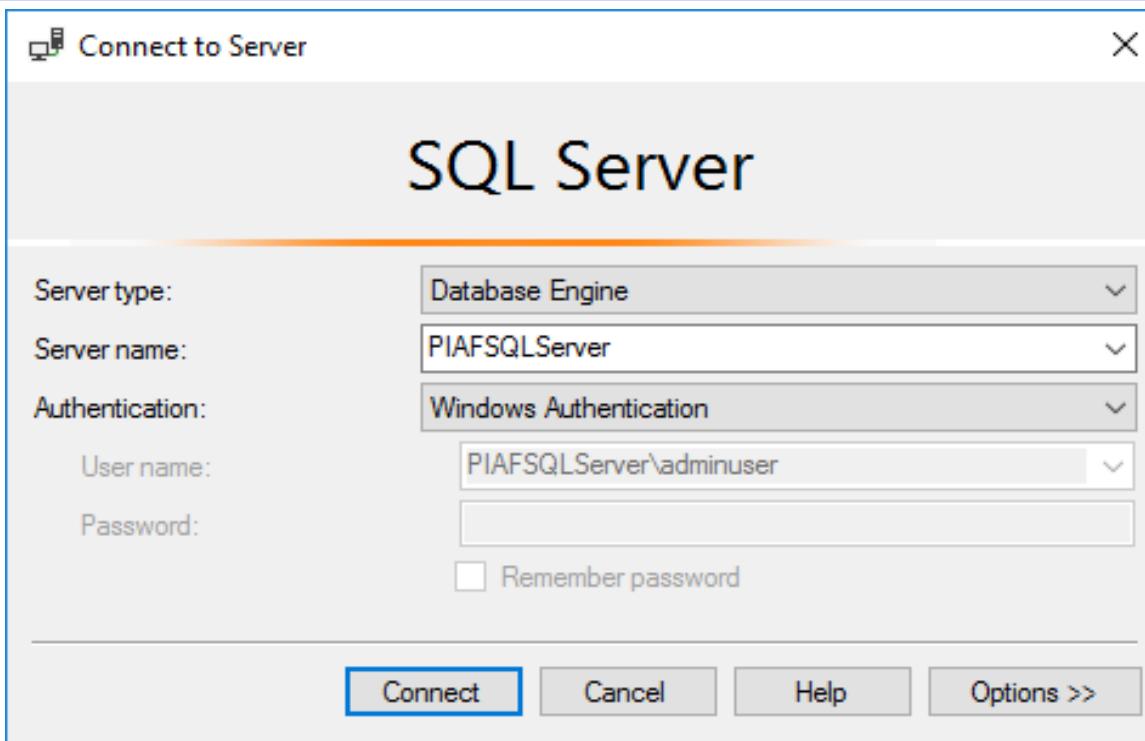
1. From the Bastion host, connect to the **PIAF** through the private IP address with the credentials provided in the output section.

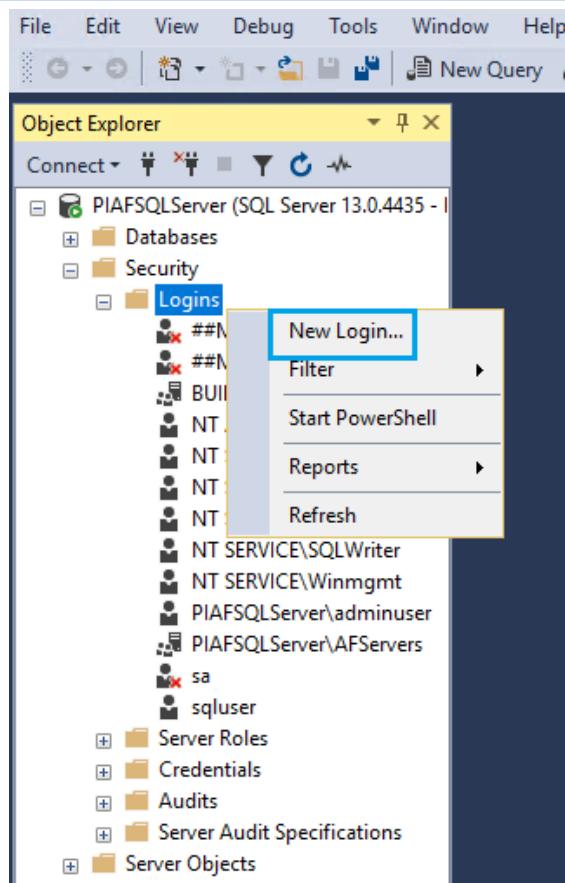
Outputs

ADMINUSERNAME	adminuser	
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com	
ADSERVERIPADDRESS	10.0.1.4	
PIAFSQLSERVERIPADDRESS	10.0.2.4	

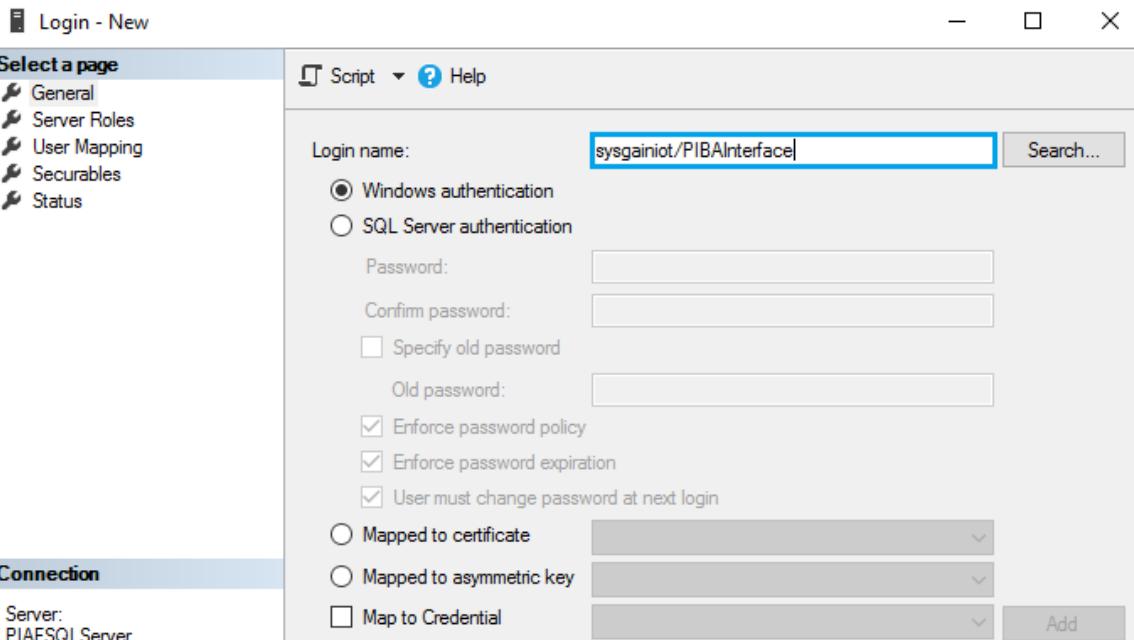


- After logging in to the PIAF SQL Server, search for **ssms** in start menu to open the **SQL Server Management Studio** and create a new login by navigating to **Security** > Right-click on **Logins** and selecting **New Login**.

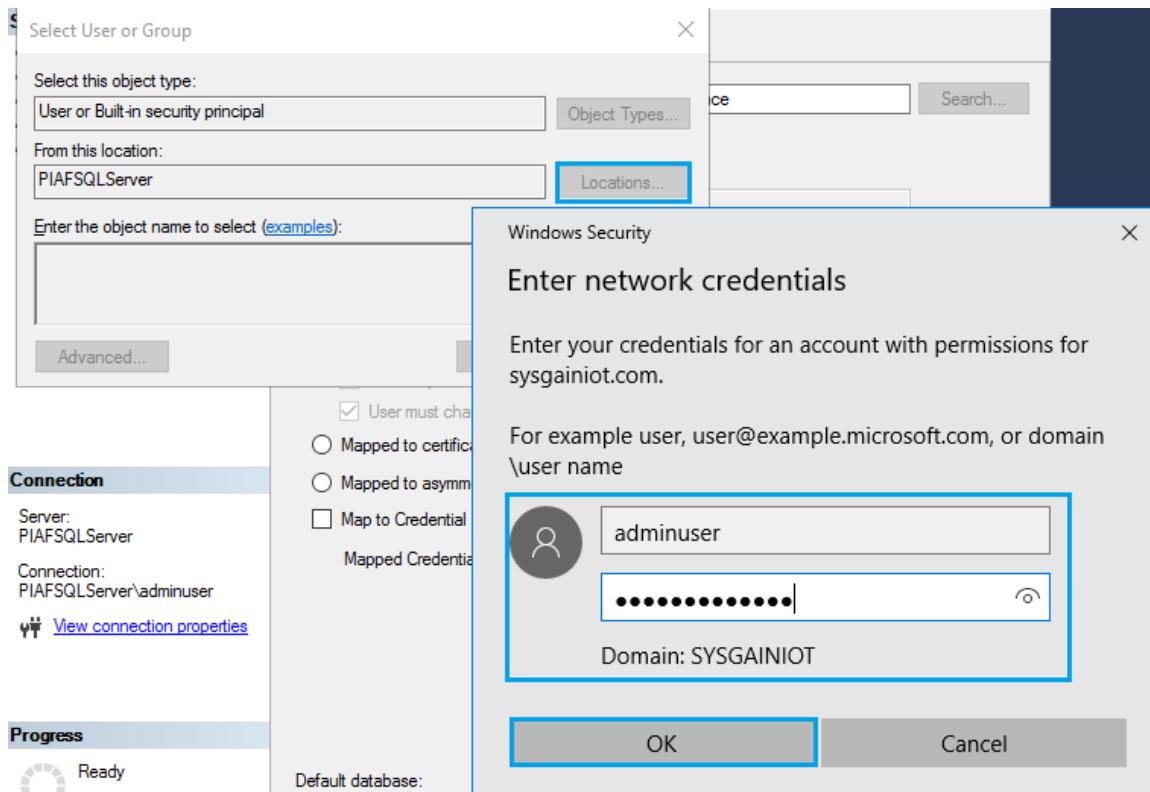




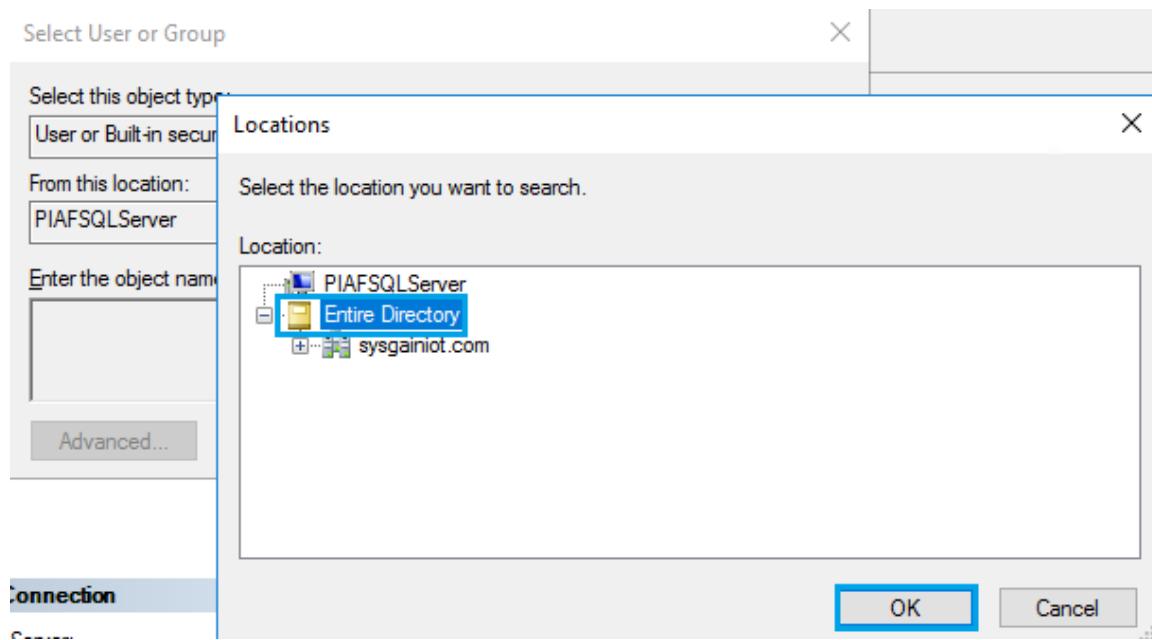
3. Give the login name as **domain name** without .com/**PIBAInterface**, then click on **Search**.



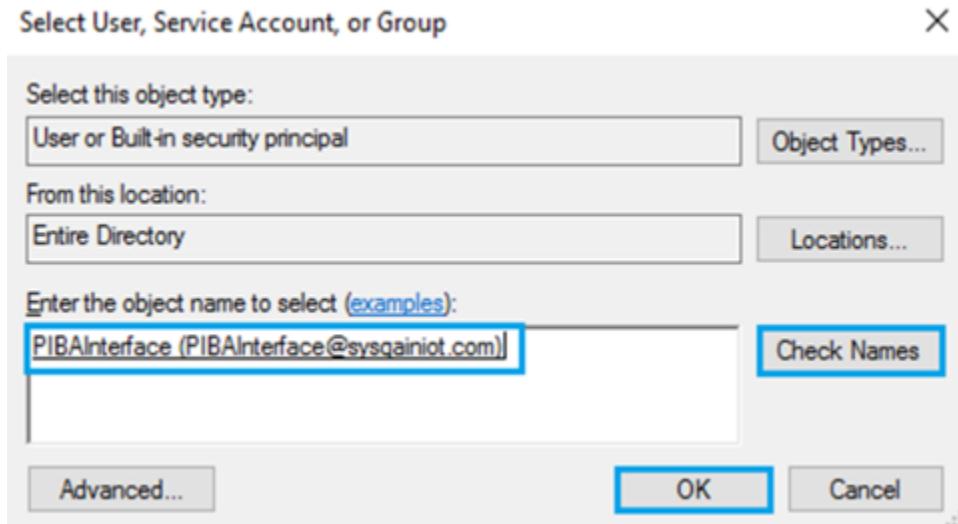
4. Click on **Locations**. You will get a popup box of credentials: enter the SQL server credentials.



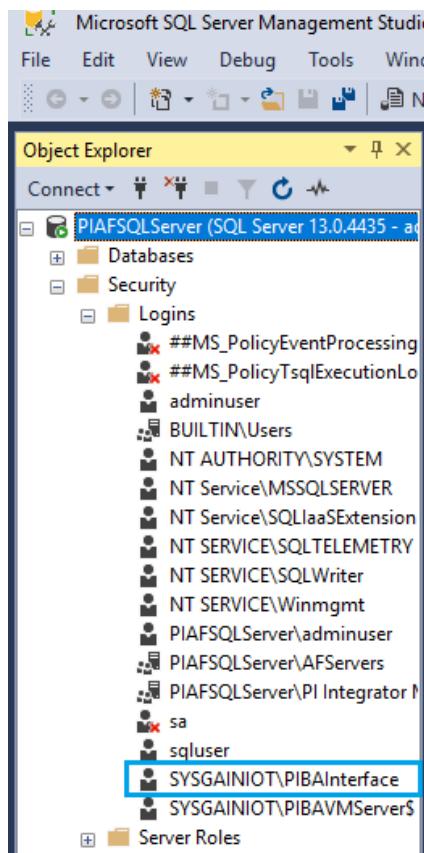
5. Select the **Entire Directory** and click on **OK**.



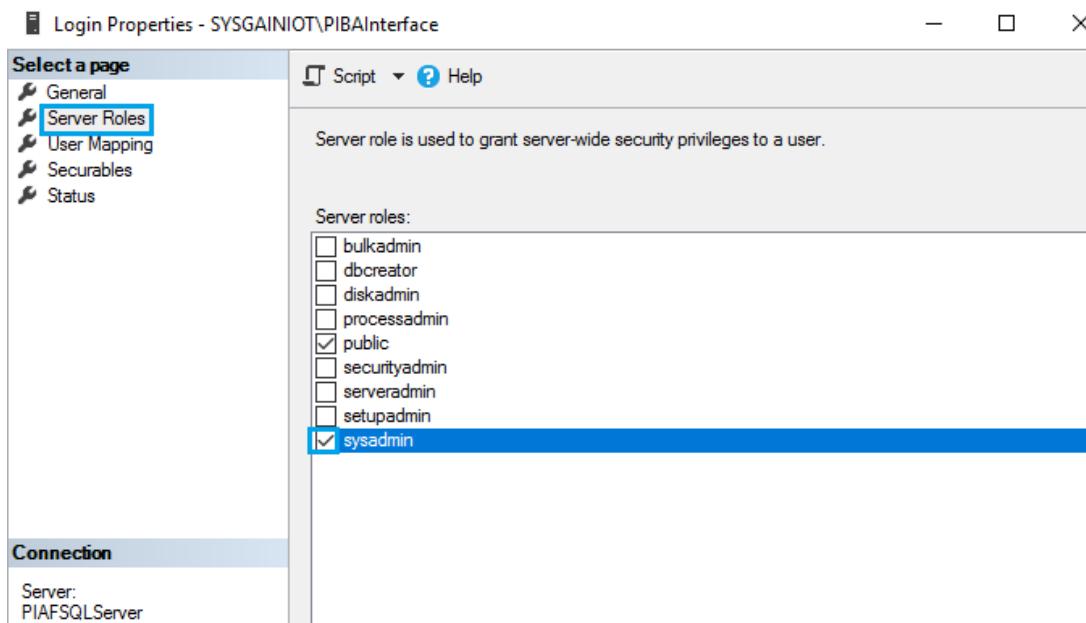
6. Enter the object name as **PIBAInterface** and click on **Check Names**. Then click on **OK**



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

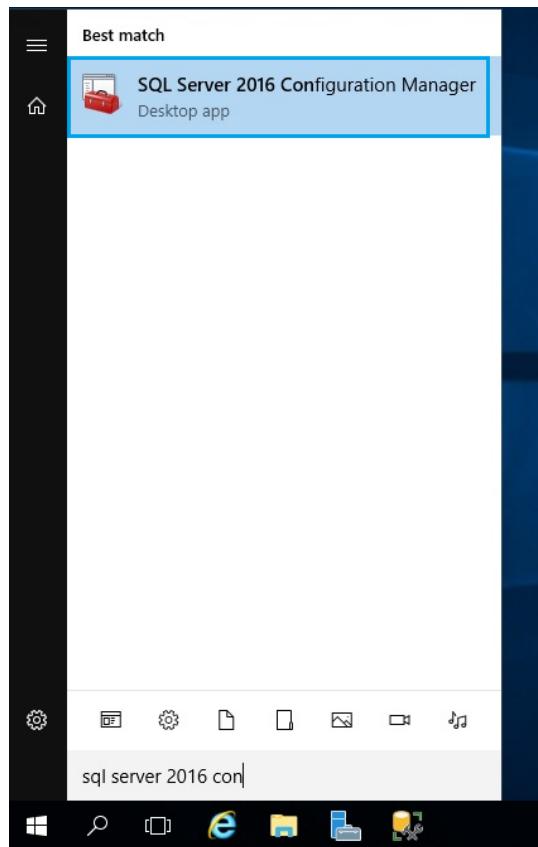


8. Right click on **User (created)** > Right click and select **properties** > click **Server Roles** > check the **sysadmin** box to give permission to the new user.

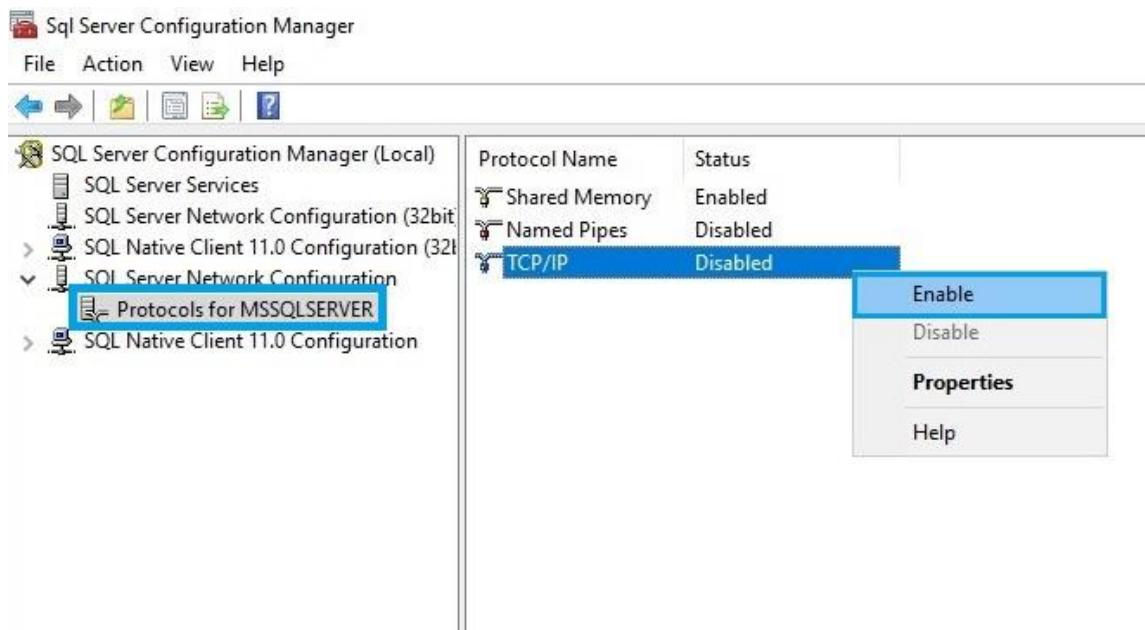


8.2. Enable TCP and Named Pipe in SQL Server Configuration Management

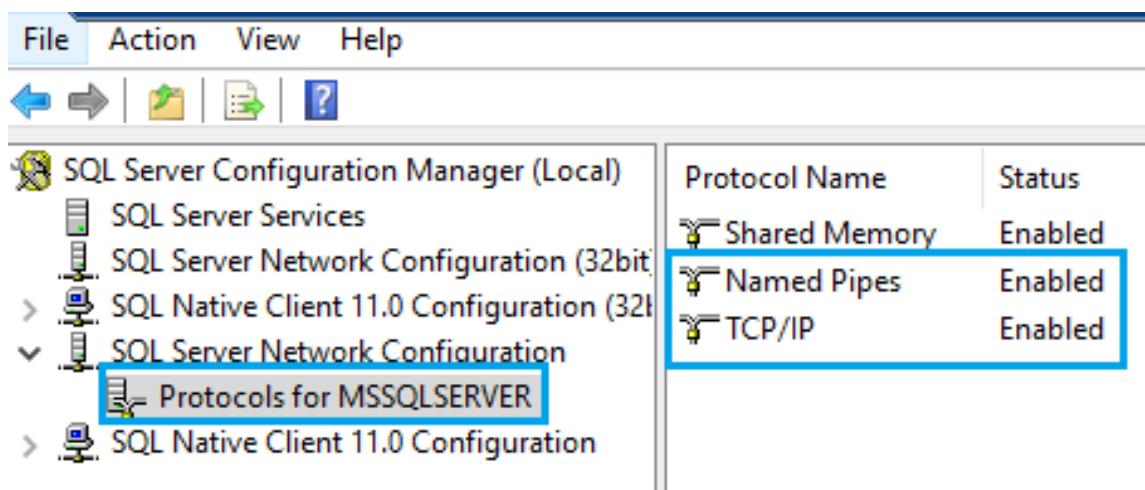
1. From the **Start** menu, navigate to **SQL Server 2016 Configuration Management**.



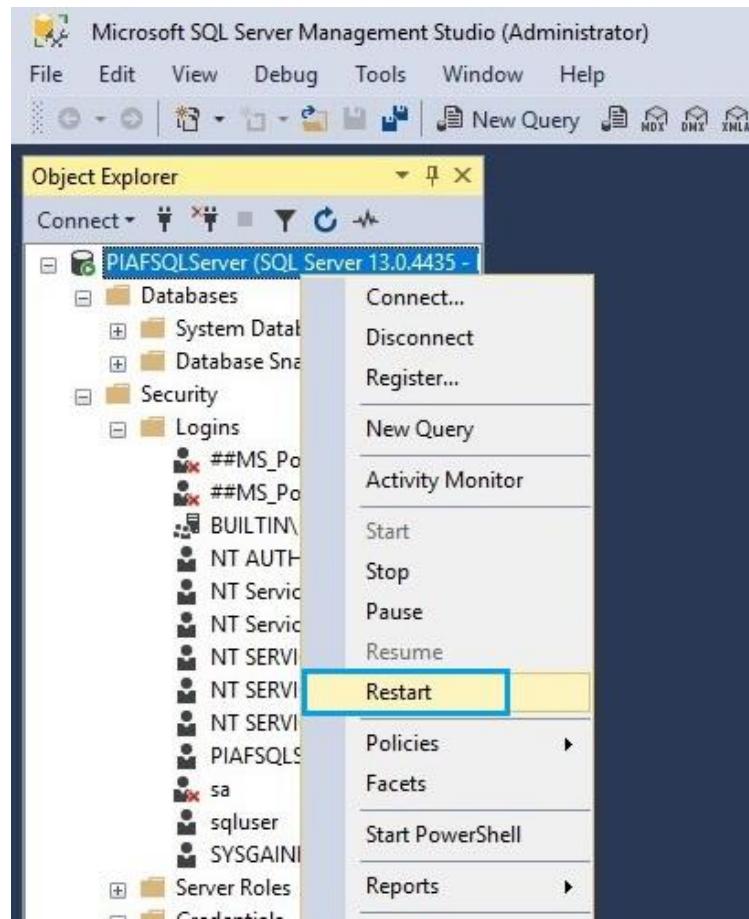
2. Click on **SQL Server Network Configuration > Protocols for MSSQLSERVER**.



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.

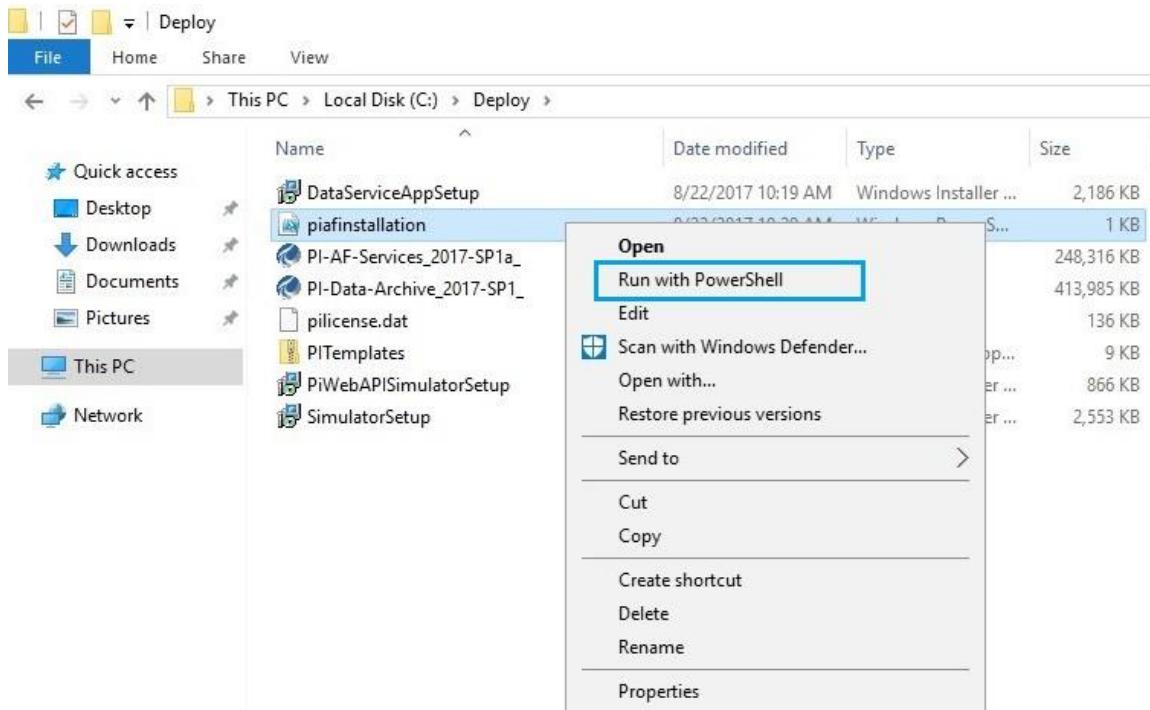
Outputs	
ADMINUSERNAME	adminuser
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com
ADSERVERIPADDRESS	10.0.1.4
PIAFSQLSERVERIPADDRESS	10.0.2.4



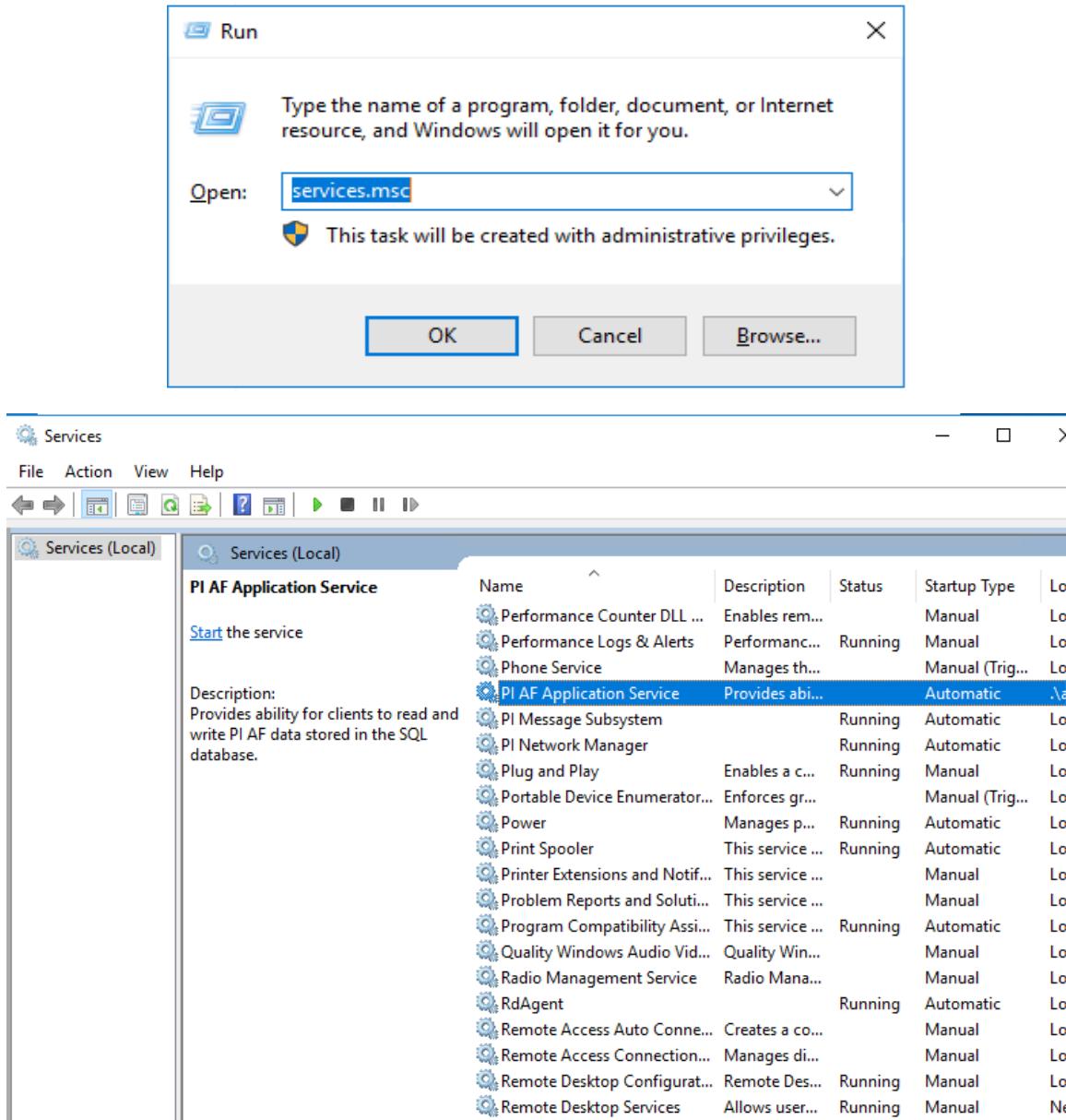
2. Navigate to **Local disk (C:) > Deploy** > Right click on **piafinstallation** > Open with Notepad. In the PowerShell script, edit the **admininuser** and **Password@1234** values to update them with your username and password from the PIAFSQLServer and then **save**. After that, right click on the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



```
C:\Deploy\PI-AF-Services_2017-SP1a_.exe ADDLOCAL=ALL AFSERVICEACCOUNT=PIAFSQLSERVER\admininuser AFSERVICEPASSWORD=Password@1234 FDSQLDBSERVER=PIAFSQLSERVER /quiet
```



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



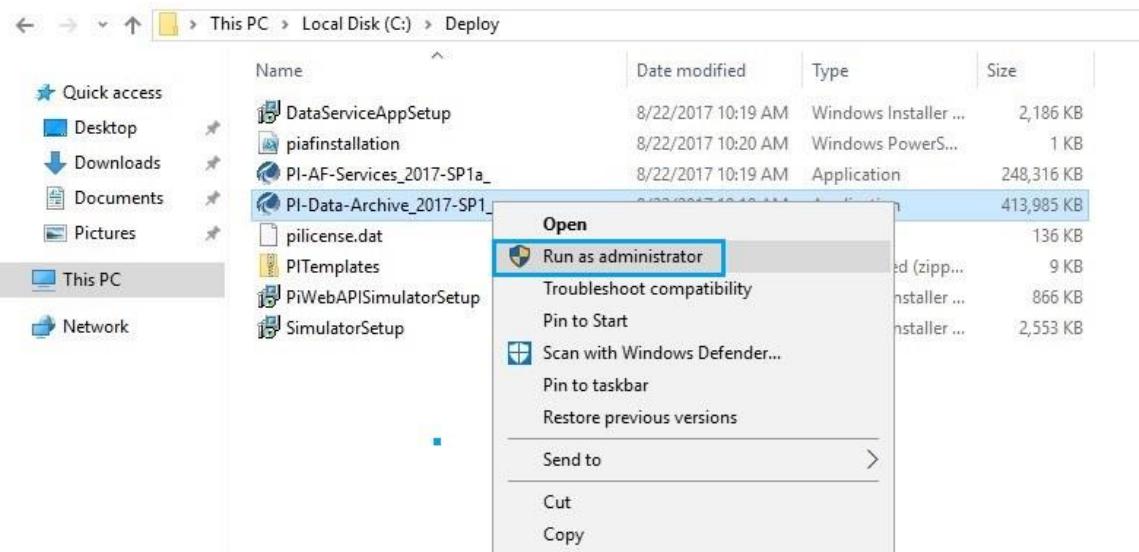
9.2. PI Data Archive (PIDA)

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.

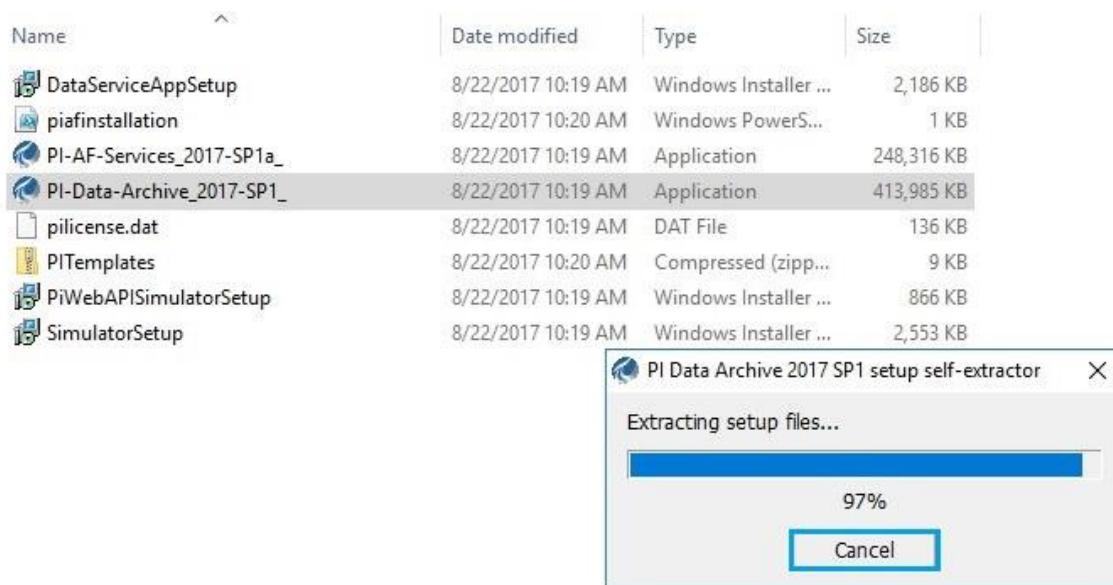
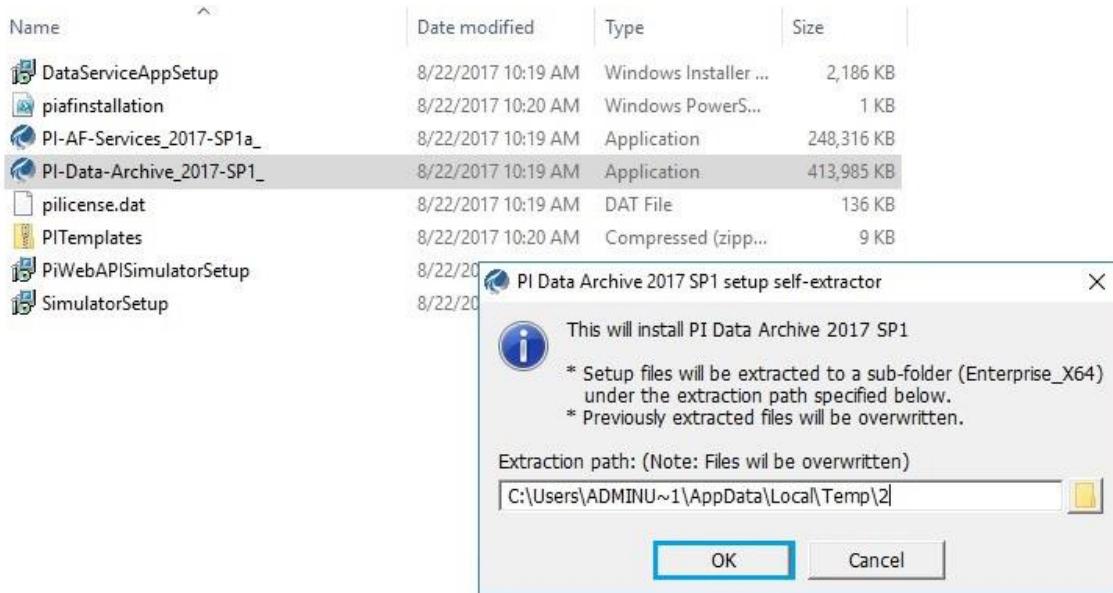
The PI Data Archive collects, stores, and organizes data from data sources, providing an information infrastructure. The PI Server also includes tools for analytics, alerts, and auditing. The PI Server may be connected to almost any existing automation, lab, or information system. Operators, engineers, 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)

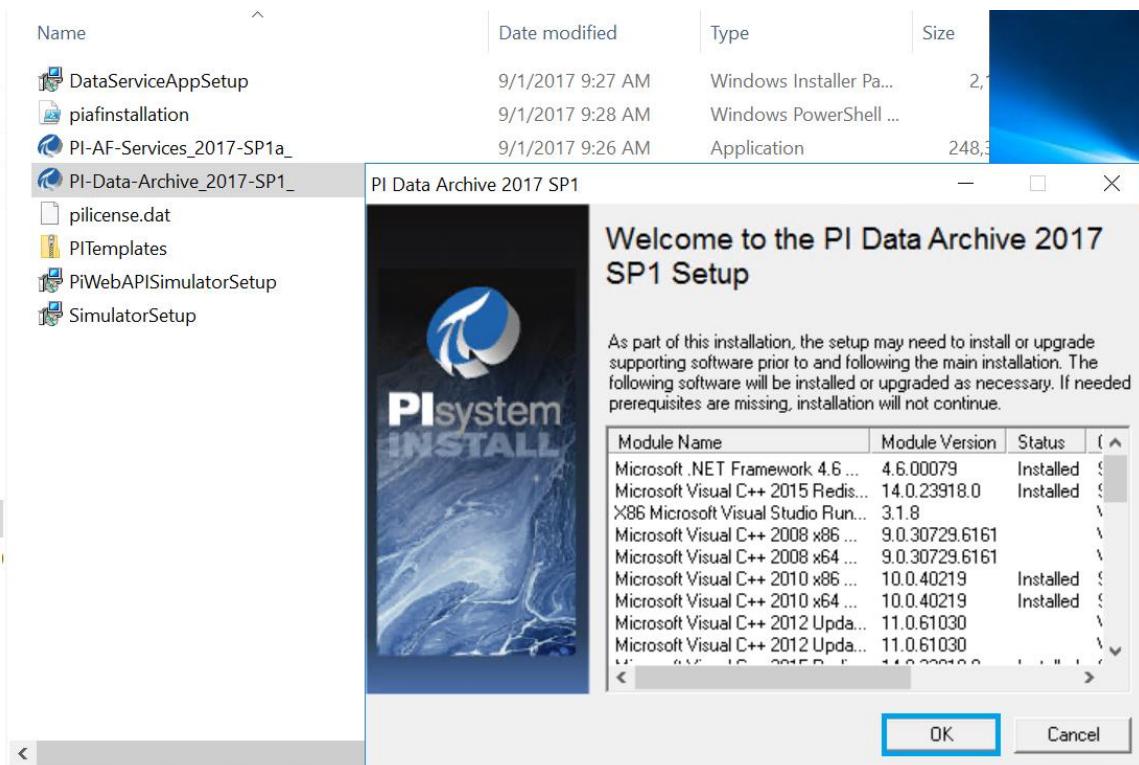
1. Navigate to **Local disk (C:)** > **Deploy** > select **PI-Data-archive_2017-SP1** > right click and **Run as administrator**.



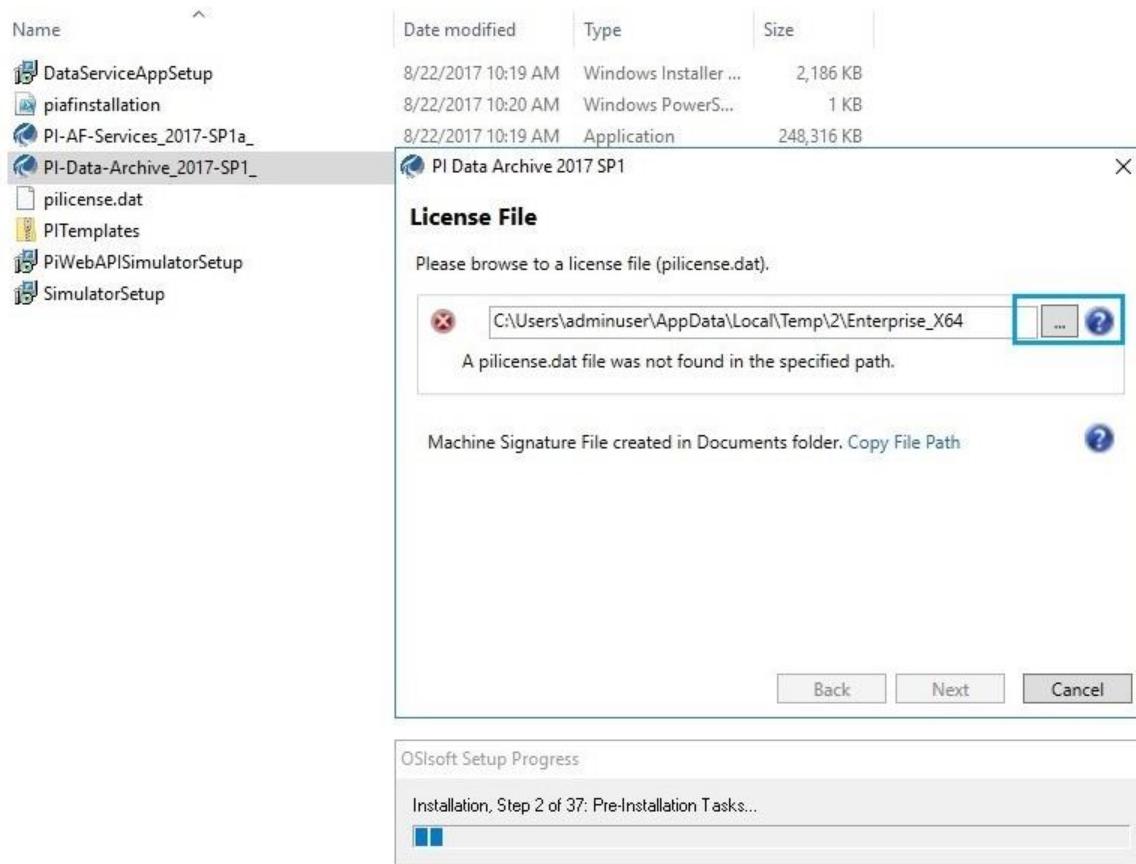
2. Click on **OK**.



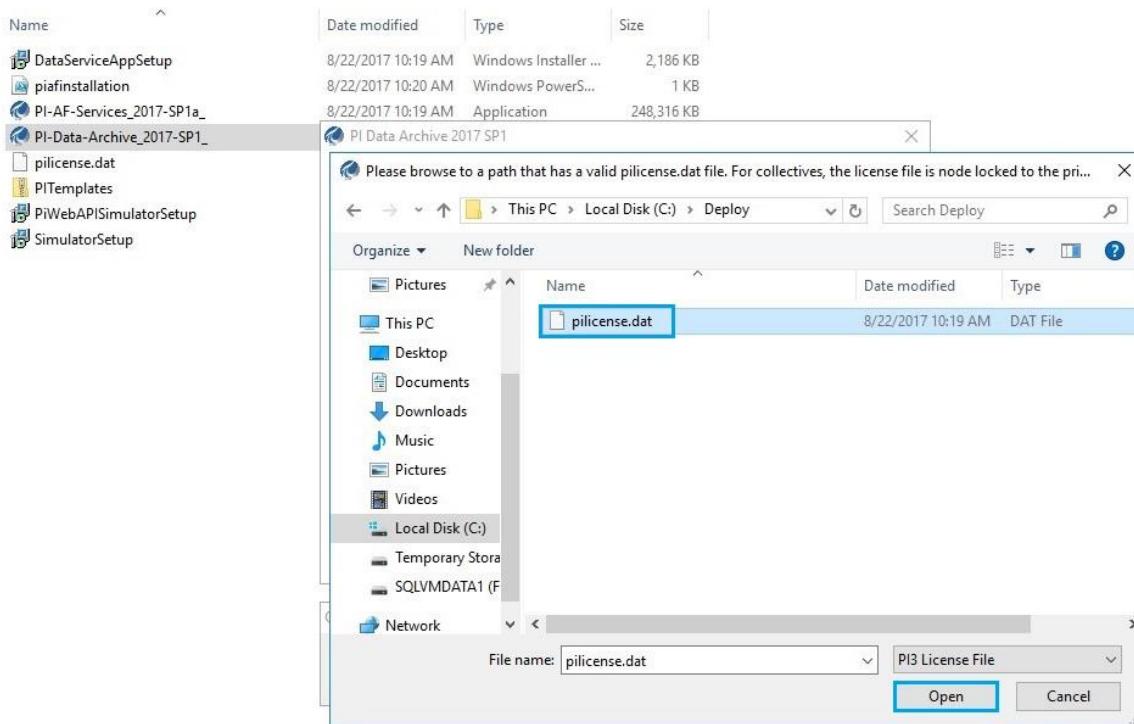
3. Click on **OK**.



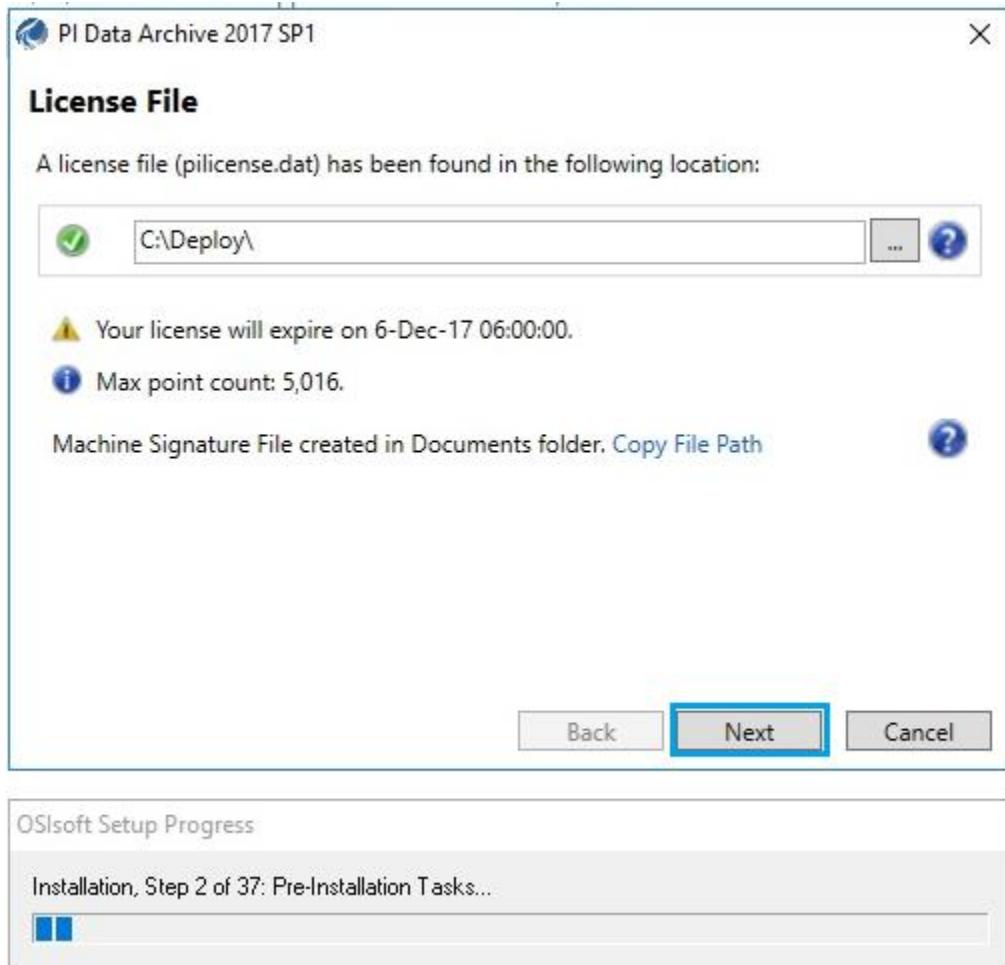
4. After completion of extracting setup files, click on **OK**.



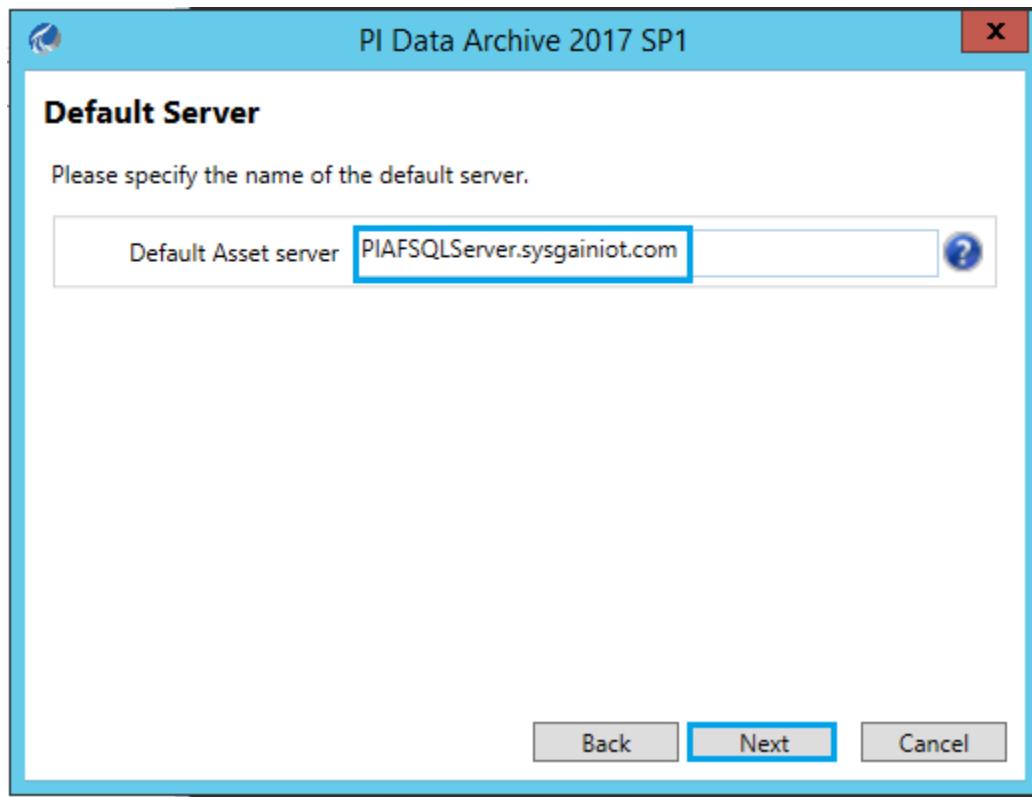
5. Click on the browse option, then navigate to the **Local disk (C:) > Deploy** > select **pilicense.dat** and click on **Open**.



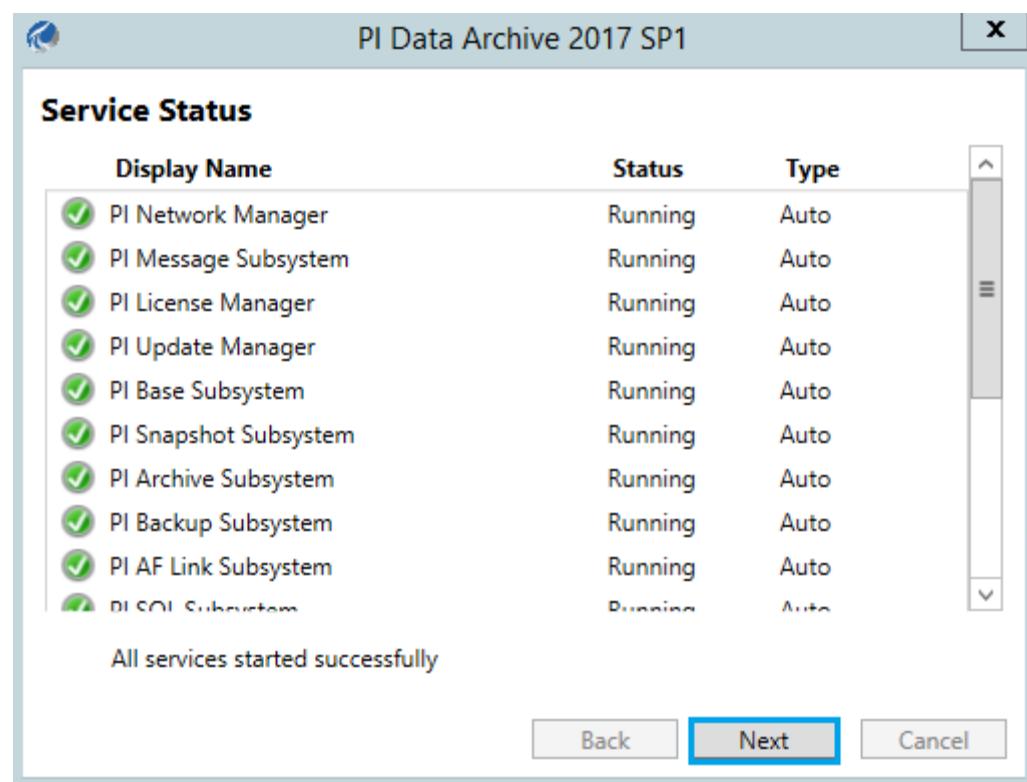
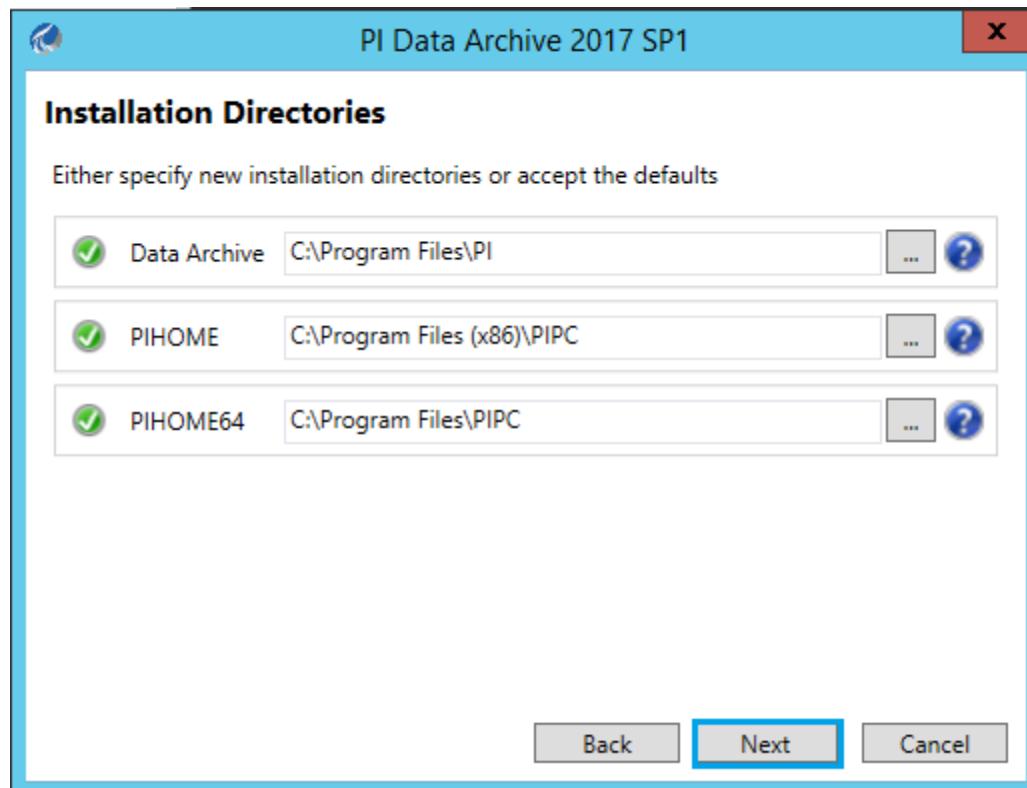
6. After that, click on **Next**.



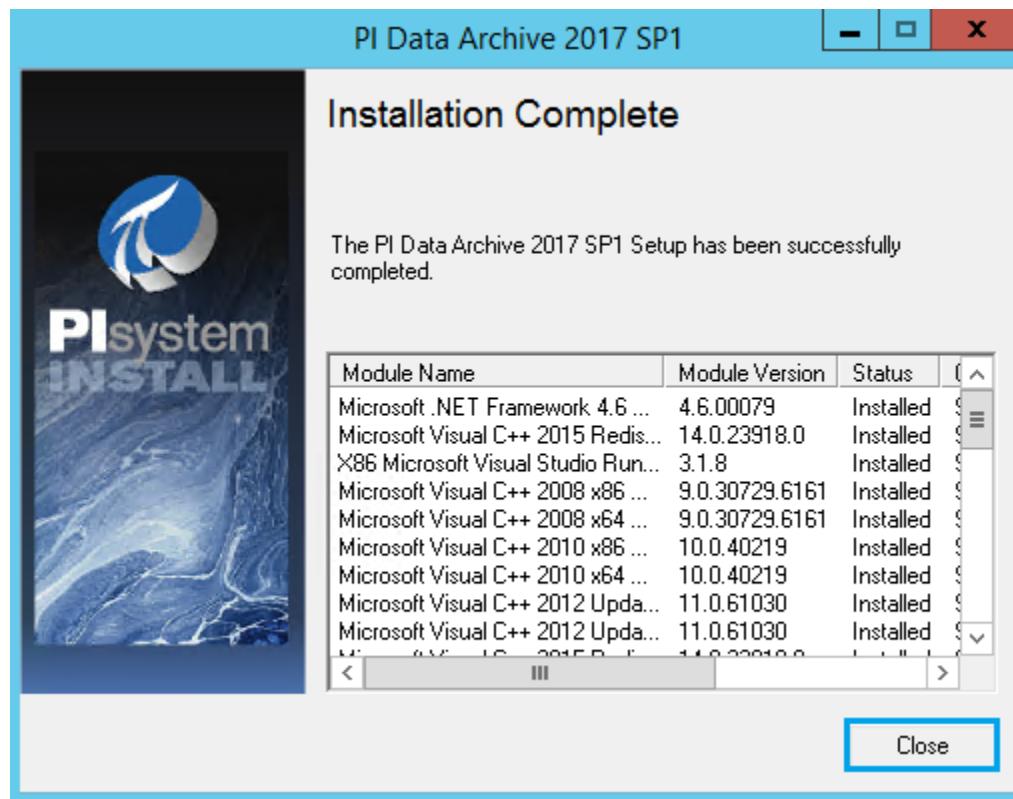
-
7. Add the domain name to the **Default Asset server** and click on **Next**.



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

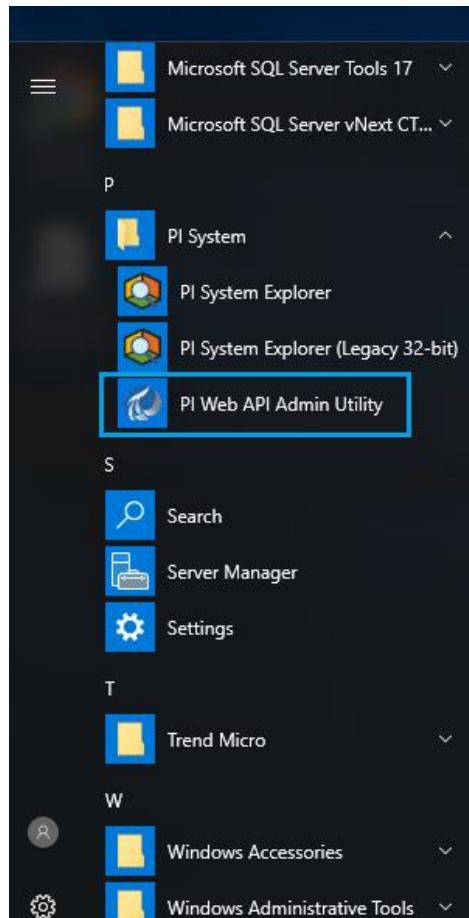


9. Click on **Close** once the installation is completed.



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**.

Change PI Web API Installation Configurations

PI System Customer Experience Improvement Program

► Telemetry

- Configuration Store
- Listen Port
- Certificate
- API Service
- Crawler Service
- Submit Url
- Review Changes
- Progress
- Confirmation

This software includes a feature that collects anonymous usage data. OSIsoft uses the collected data to improve the PI System and to prioritize new features. The collected data does not include business data or logic, but may include identifying information, such as IP addresses, host names, and names of PI System objects.

Would you like to enable the data collection feature and participate in the PI System Customer Experience Improvement Program?

Yes, I would like to participate.

Back

Next

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

Change PI Web API Installation Configurations

Select Operating Configuration Store

✓ Telemetry

- Configuration Store
- Listen Port
 - Certificate
 - API Service
 - Crawler Service
 - Submit Url
 - Review Changes
 - Progress
 - Confirmation

PI Web API requires space in the Configuration database on a PI Asset Server (AF Server). This space allows PI Web API to store operating configurations and persist other data relevant to the operation of PI Web API. You must be an Administrator on the selected Asset Server in order to proceed.

Select the Asset Server on which to create the configuration instance:

 PIAFSQLServer ... Connect

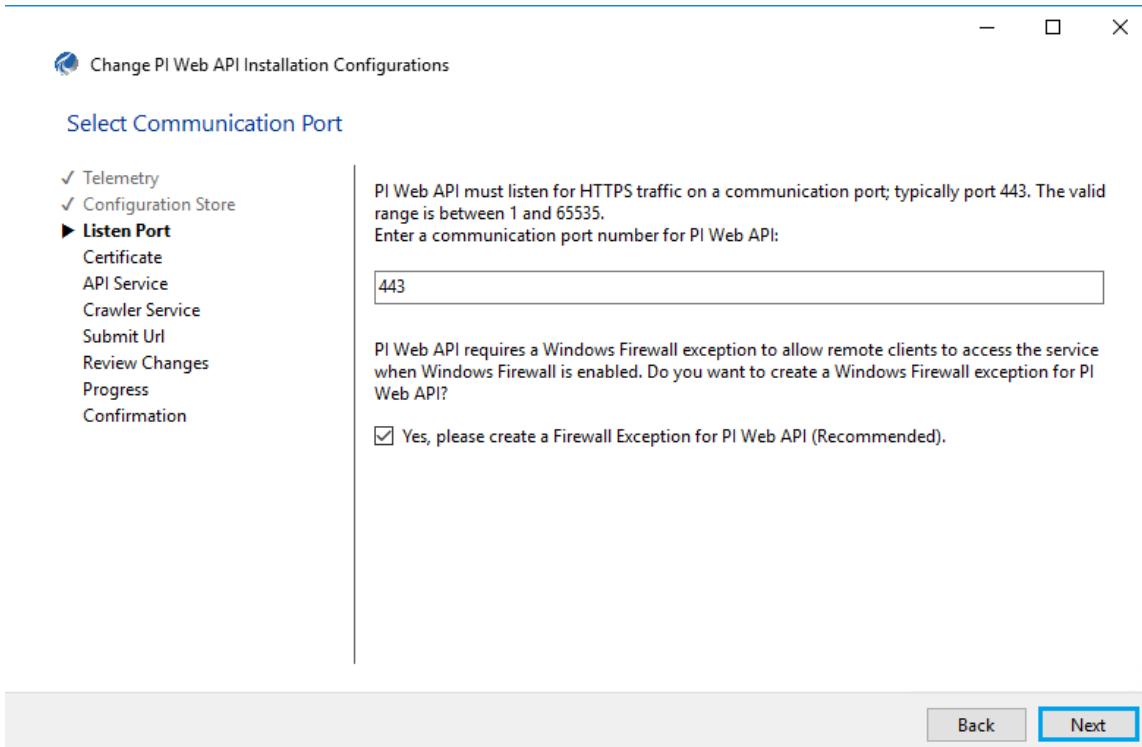
Enter the name of the instance to create:

PIAFSQLServer

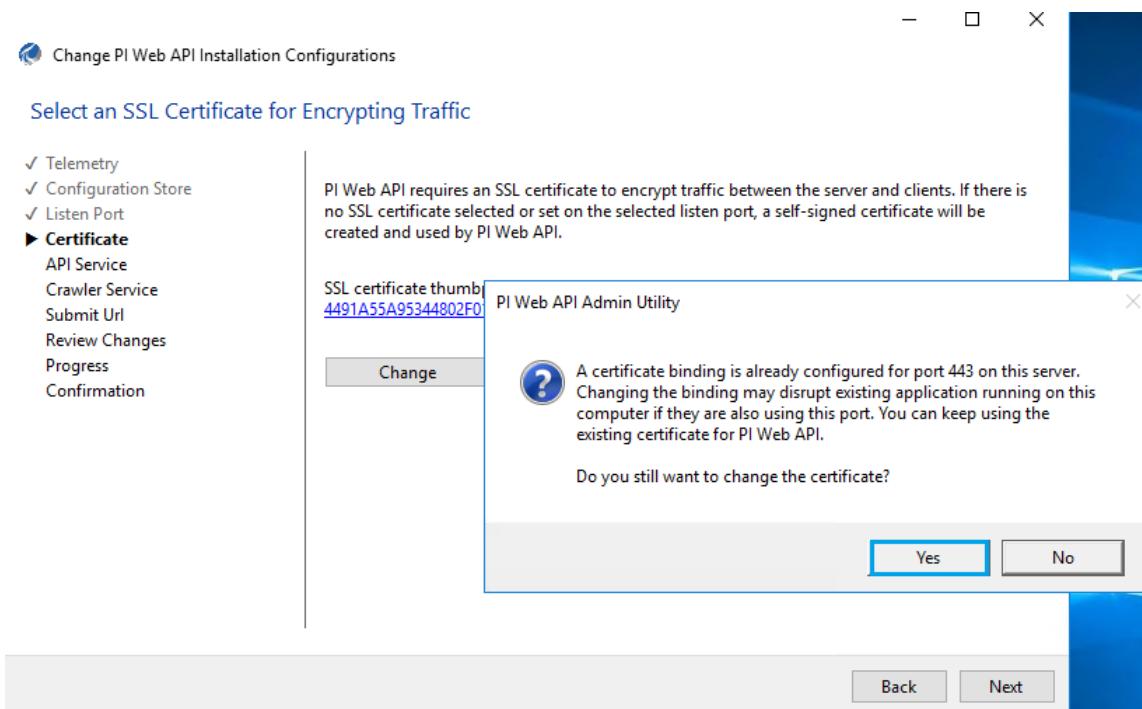
Back

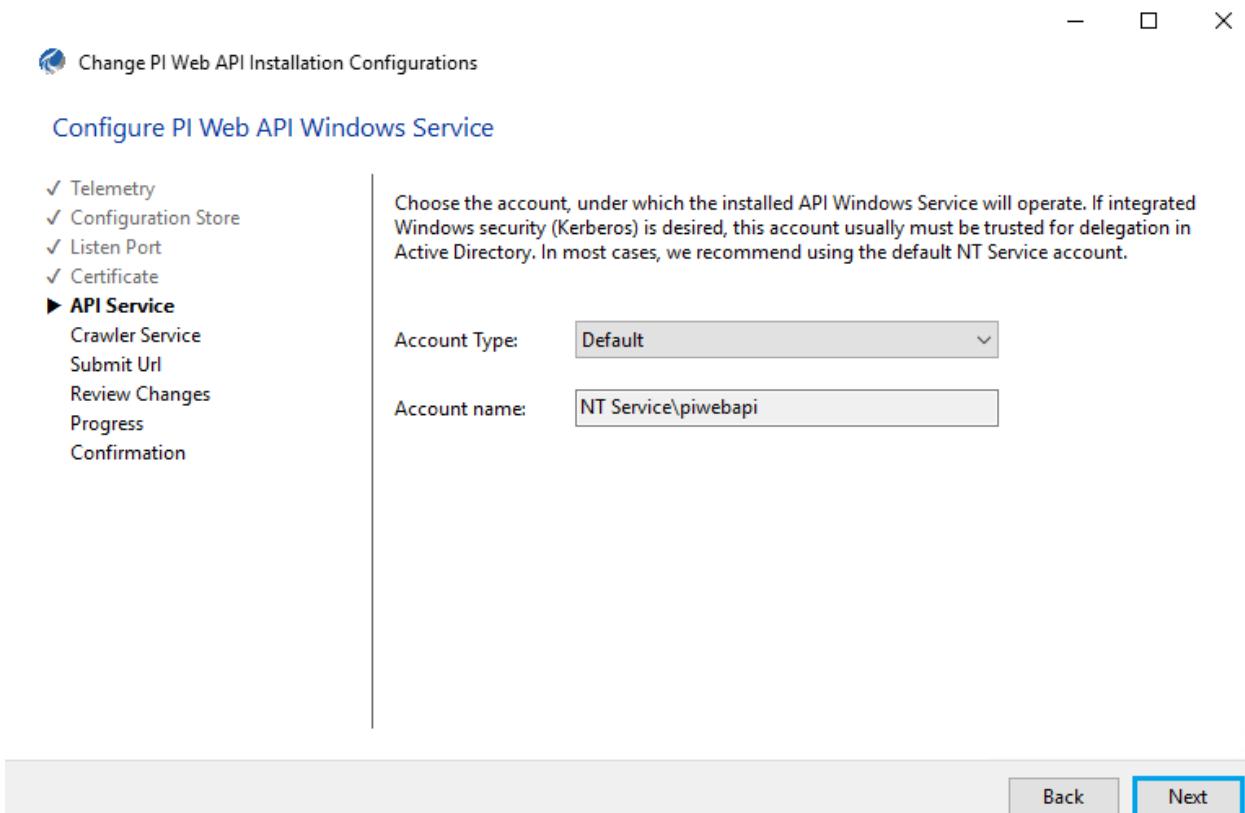
Next

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**.

Change PI Web API Installation Configurations

Configure PI Web API Windows Service

✓ Telemetry
✓ Configuration Store
✓ Listen Port
✓ Certificate
► API Service

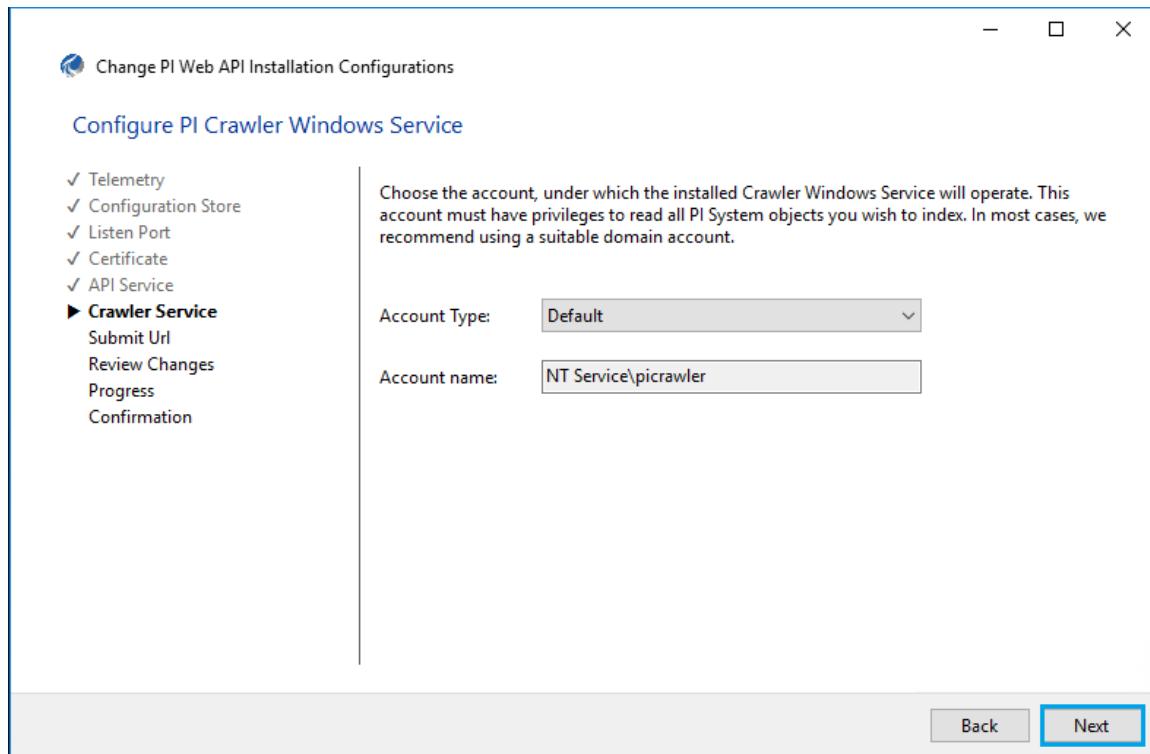
- Crawler Service
- Submit Url
- Review Changes
- Progress
- Confirmation

Choose the account, under which the installed API Windows Service will operate. If integrated Windows security (Kerberos) is desired, this account usually must be trusted for delegation in Active Directory. In most cases, we recommend using the default NT Service account.

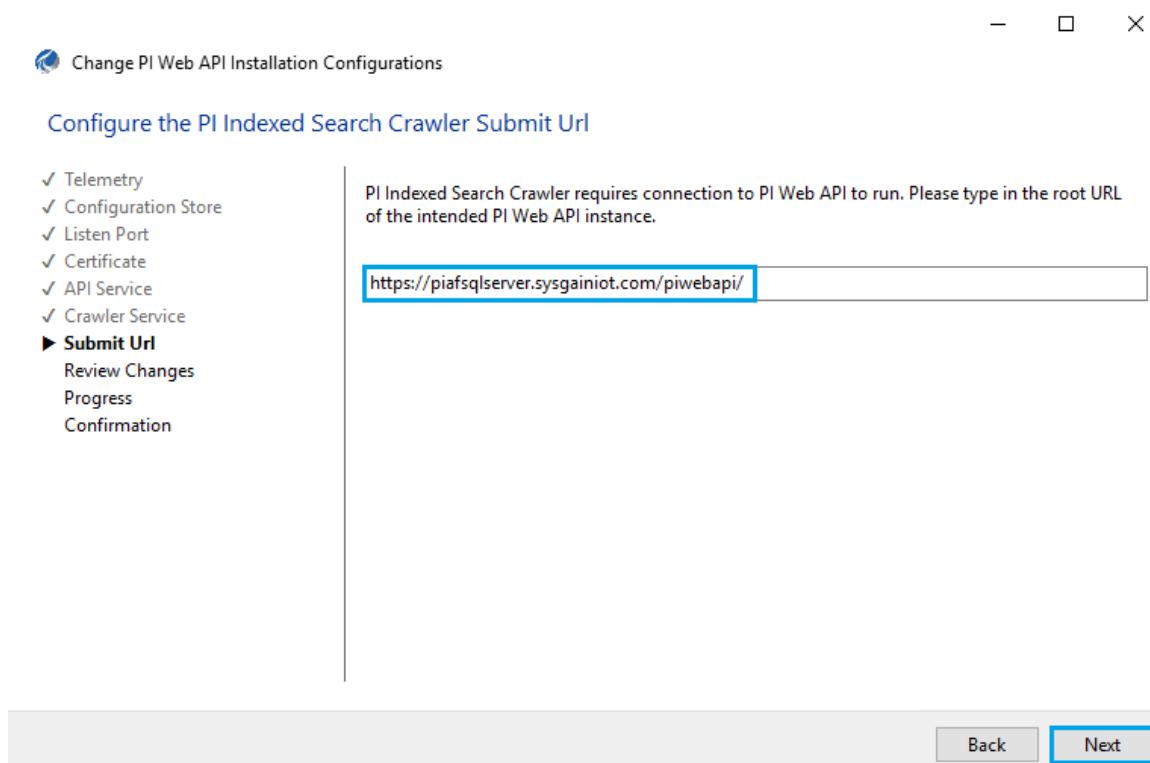
Account Type: Default

Account name: NT Service\piwebapi

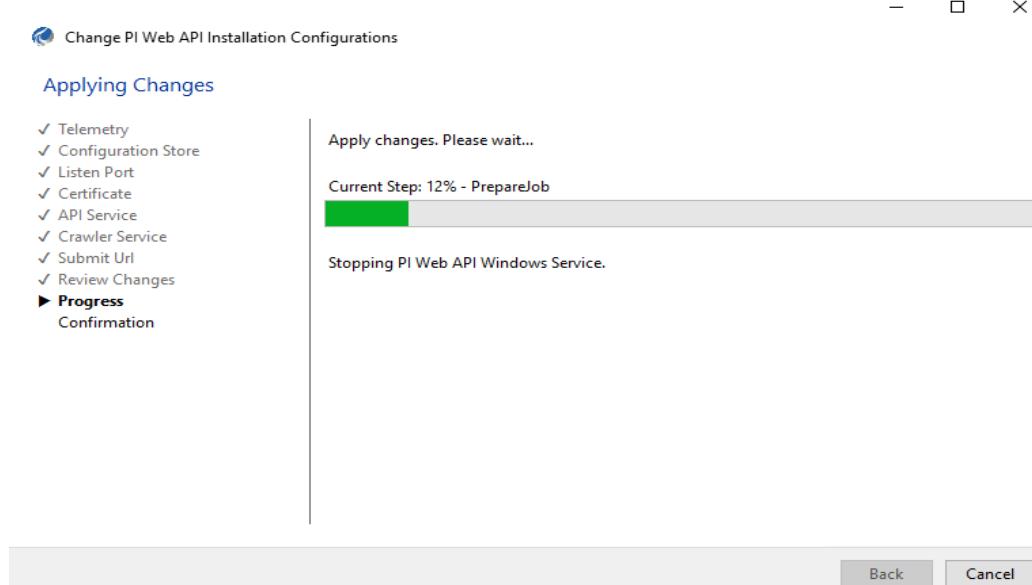
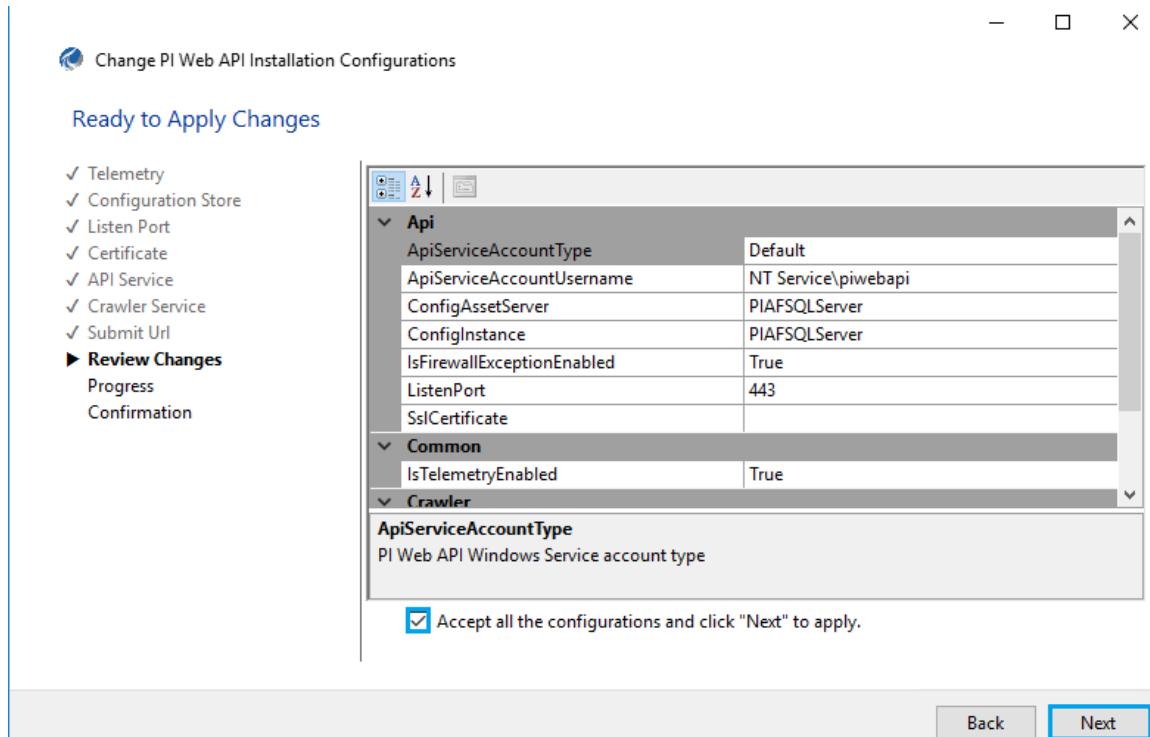
Back Next



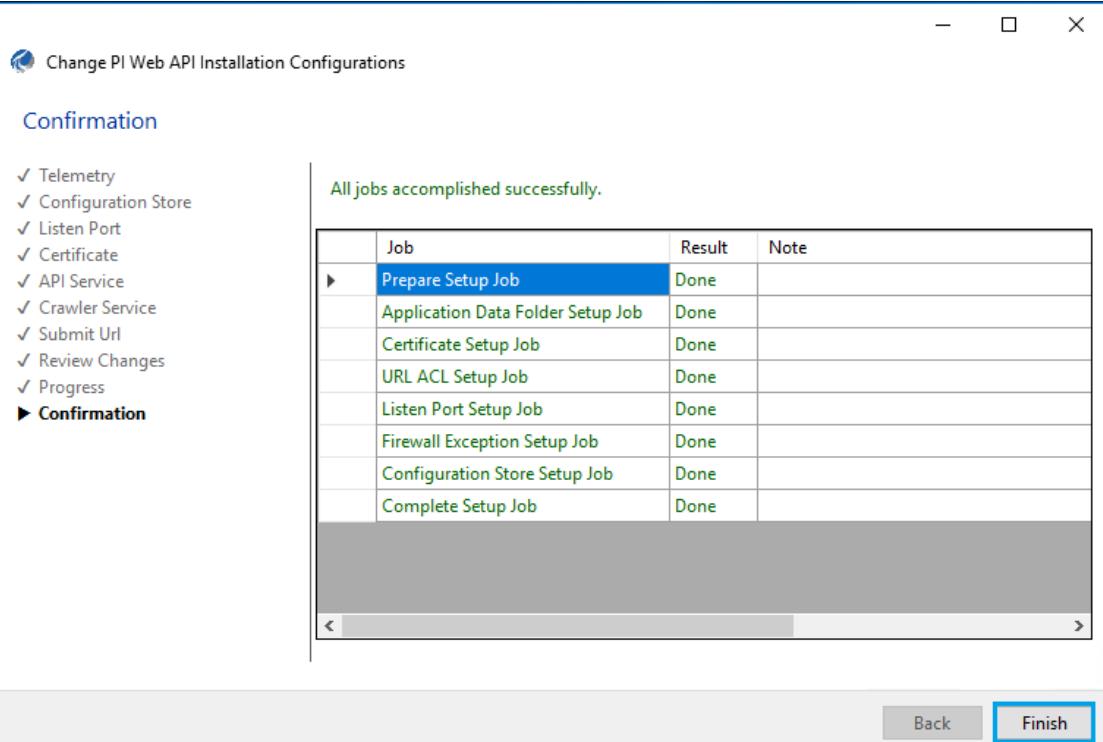
7. Note down the **Submit URL** which will be in later section



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

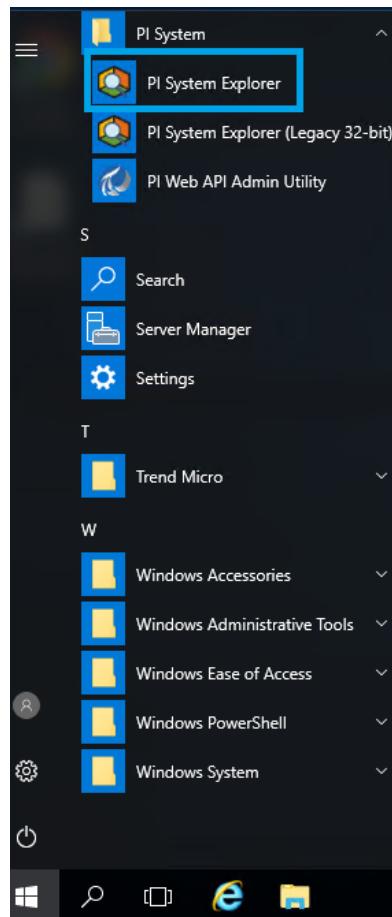


9. Click on **Finish**.

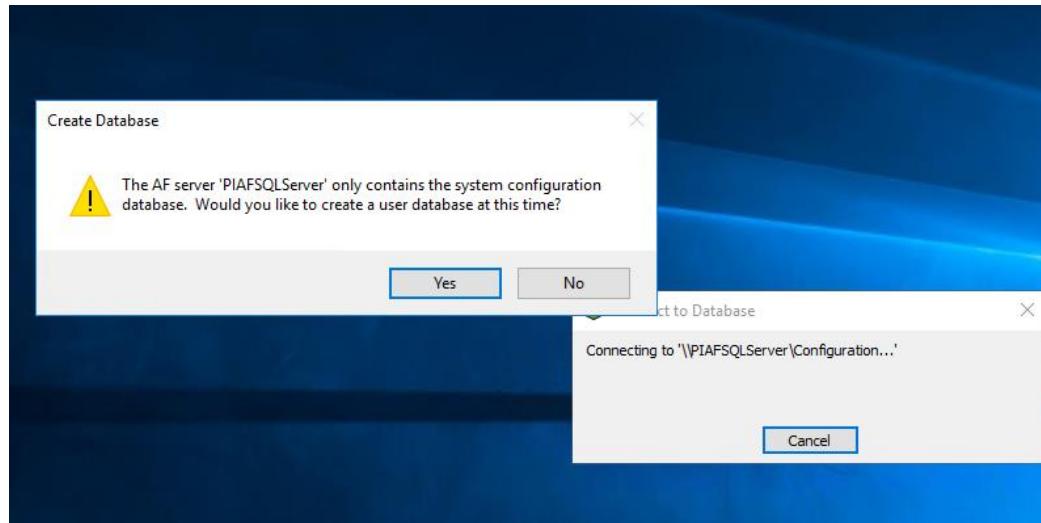


9.4. Creation of Database in PI System Explorer

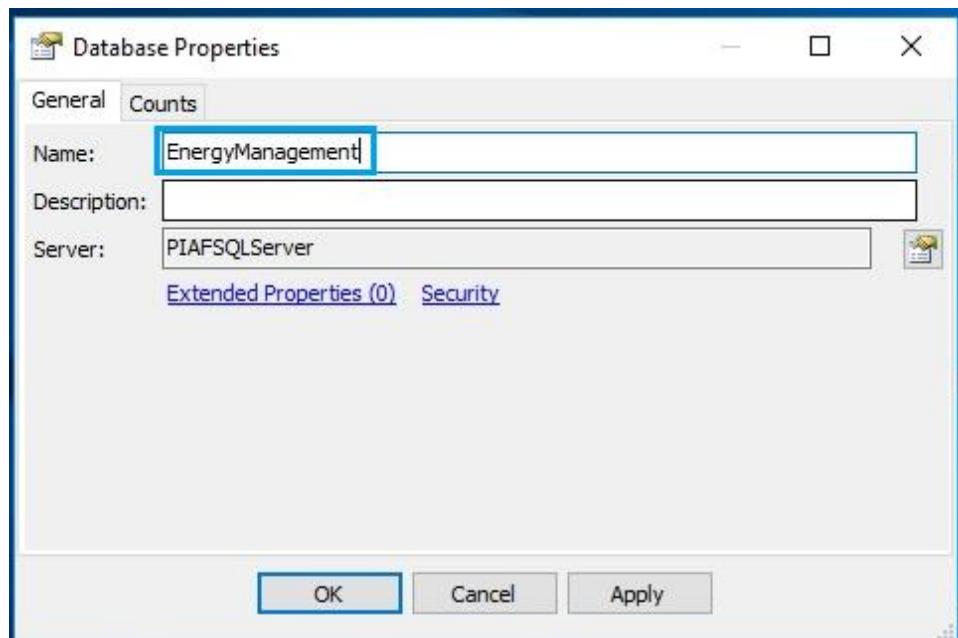
18. On the PIAFSQL machine, Navigate to **PI System Explorer** in PI System folder from the Start menu.



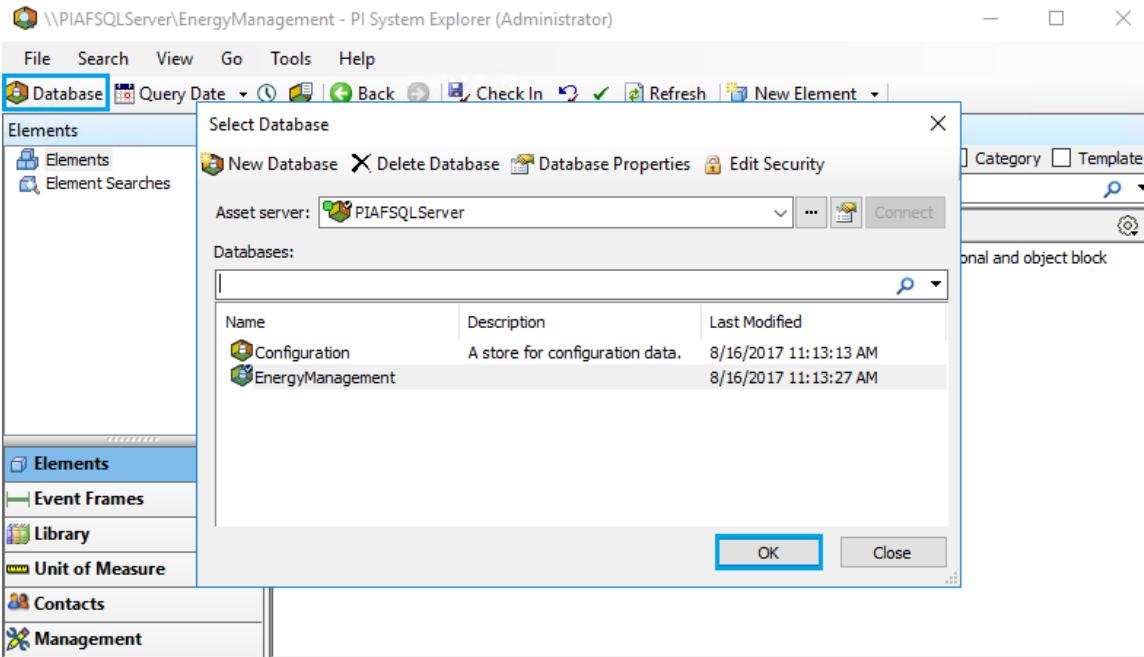
19. Two popups show up, **Connect to Database** and **Create Database**. Click **Yes** on the **Create Database** popup.



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

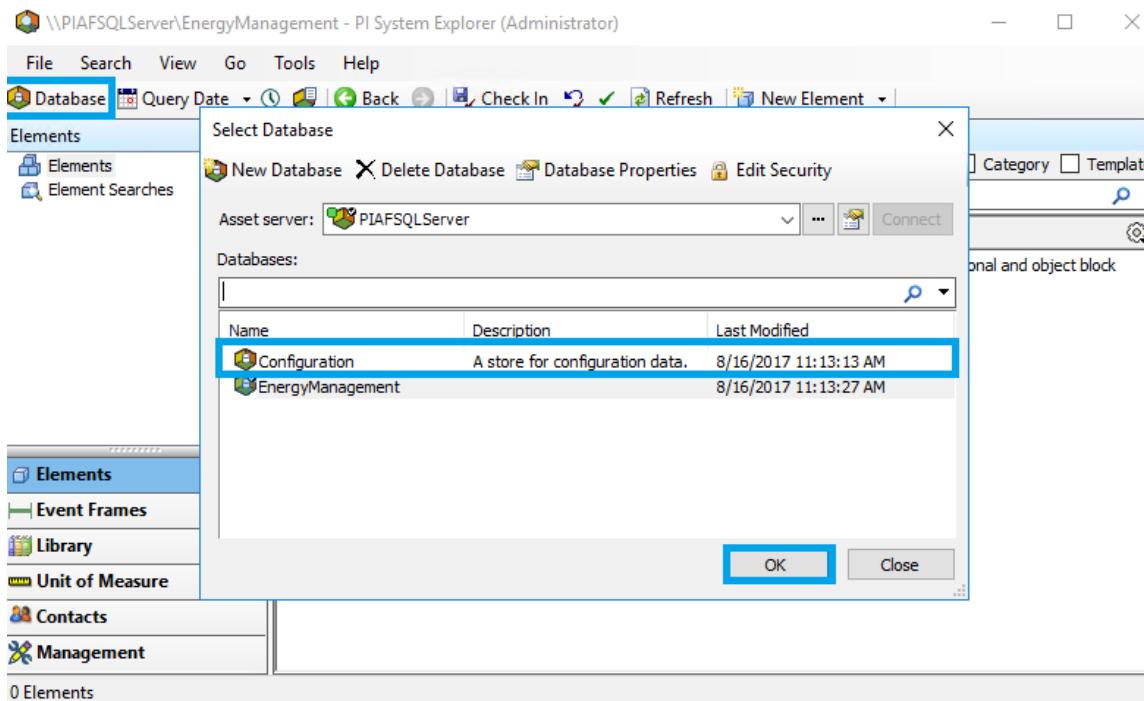


21. Navigate to **PI System Explorer**, click on **Database** to view the created database and click on **OK**.

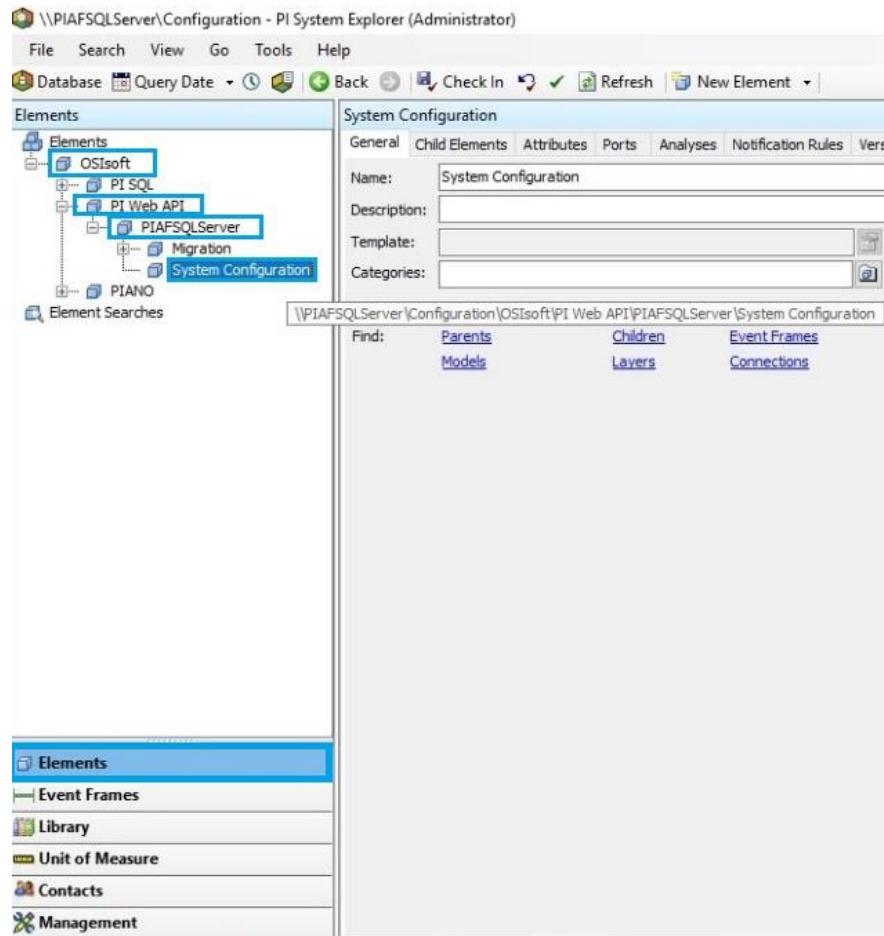


9.5. System Configuration in PI System Explorer

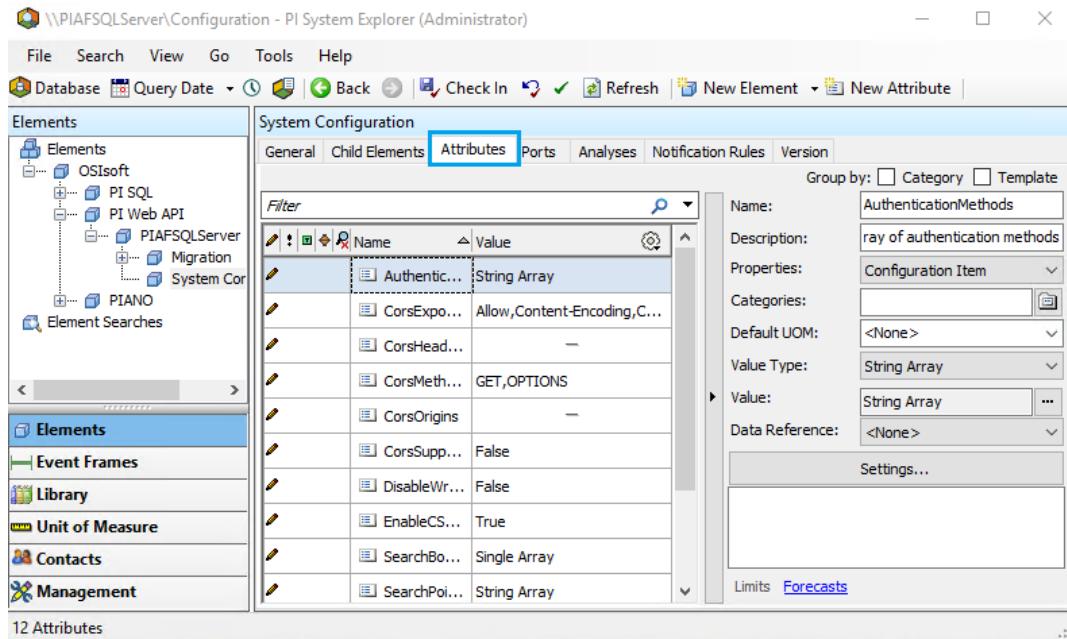
1. Navigate to **PI System Explorer** > Click on **Database** > click **Configuration** under Databases section. Click **OK**.



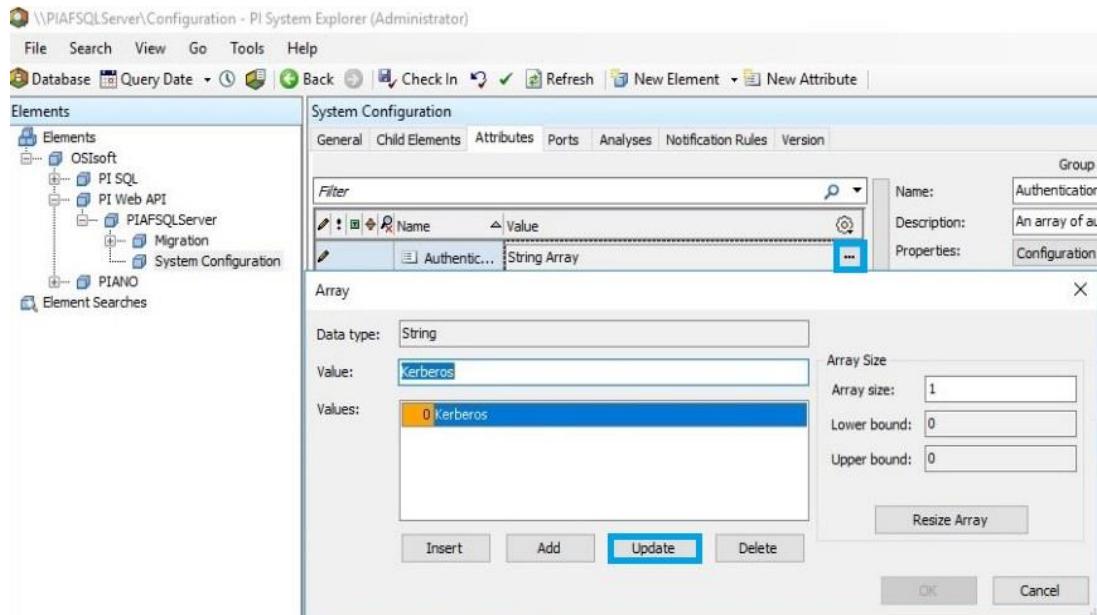
2. Click on **Elements** and navigate to **OSISoft > PI Web API > PIAFSQLServer > System Configuration**.



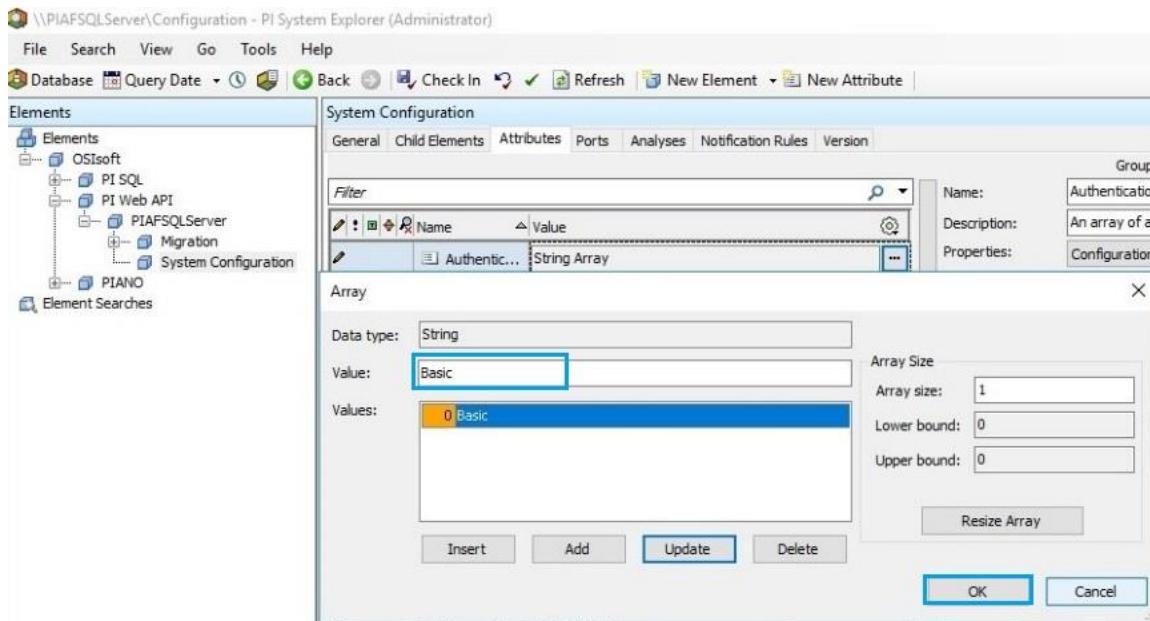
3. Click on **Attributes**.



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

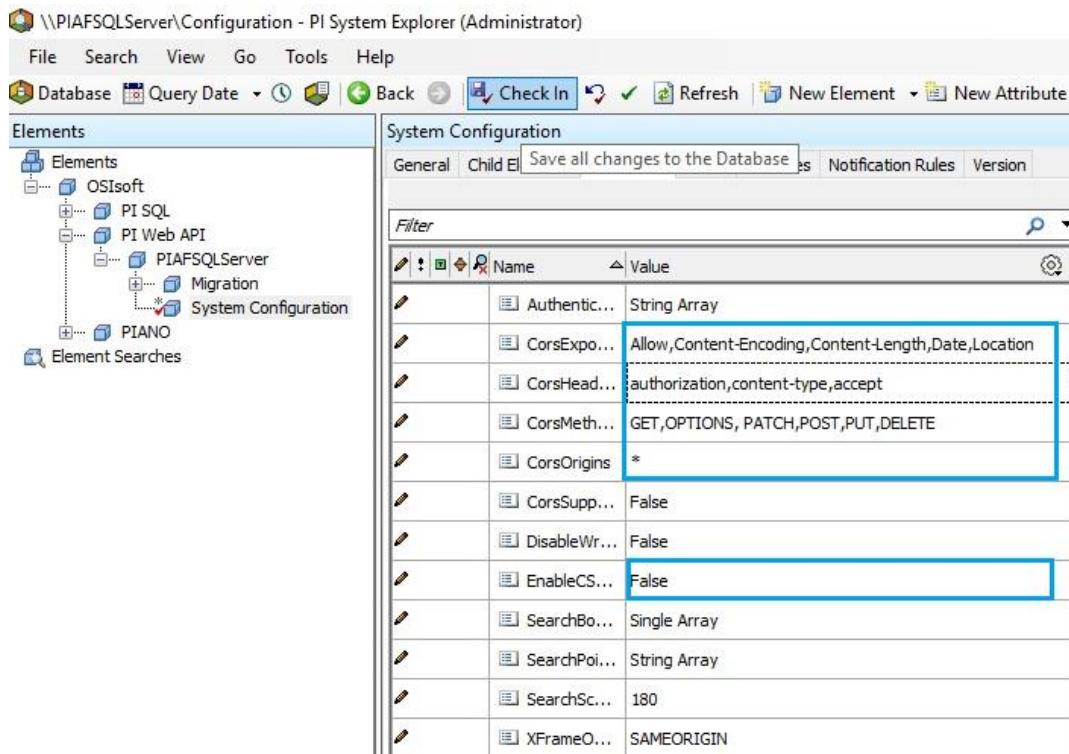


5. Click on **Update**, then **OK**.

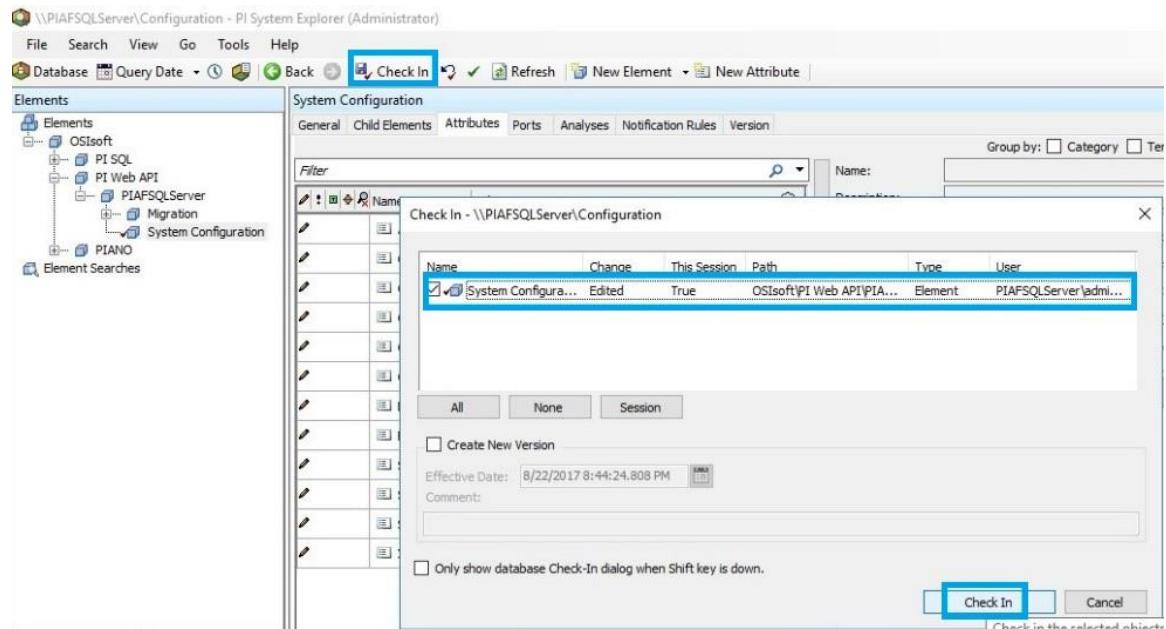


6. Similarly, change the following values:

- EnableCSRFDefense to **False**.
- Set CorsOrigins as *
- Corsmethods as **GET, OPTIONS, PATCH, PUT, POST, DELETE**
- CorsHeaders as **authorization,content-type,accept**

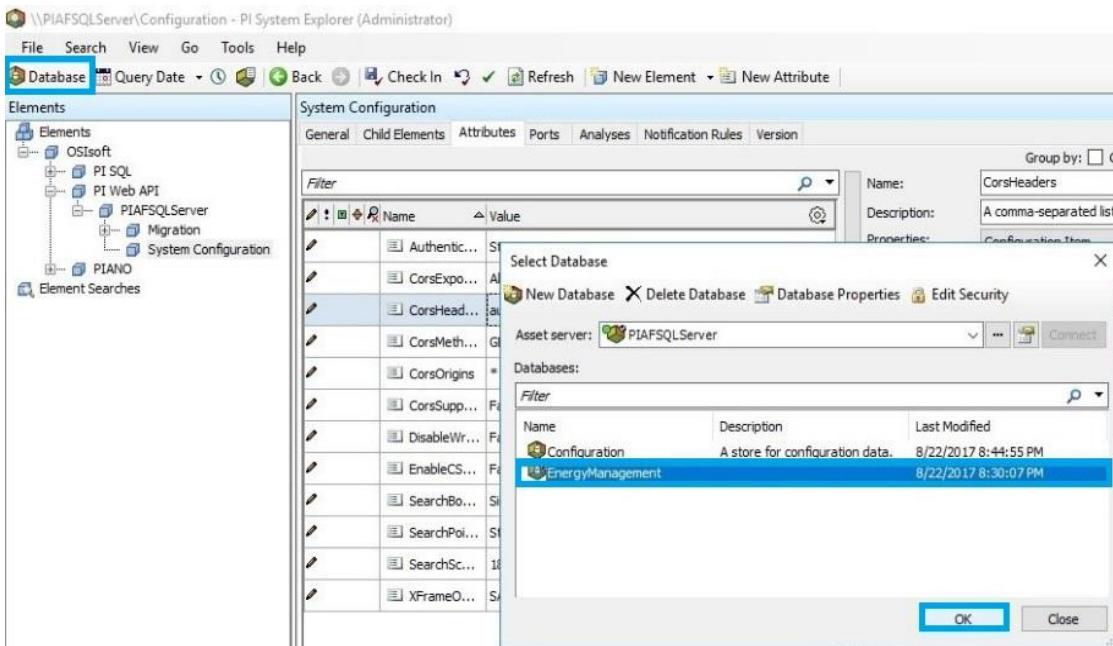


7. Select the **System Configuration** again and click on **Check In**.

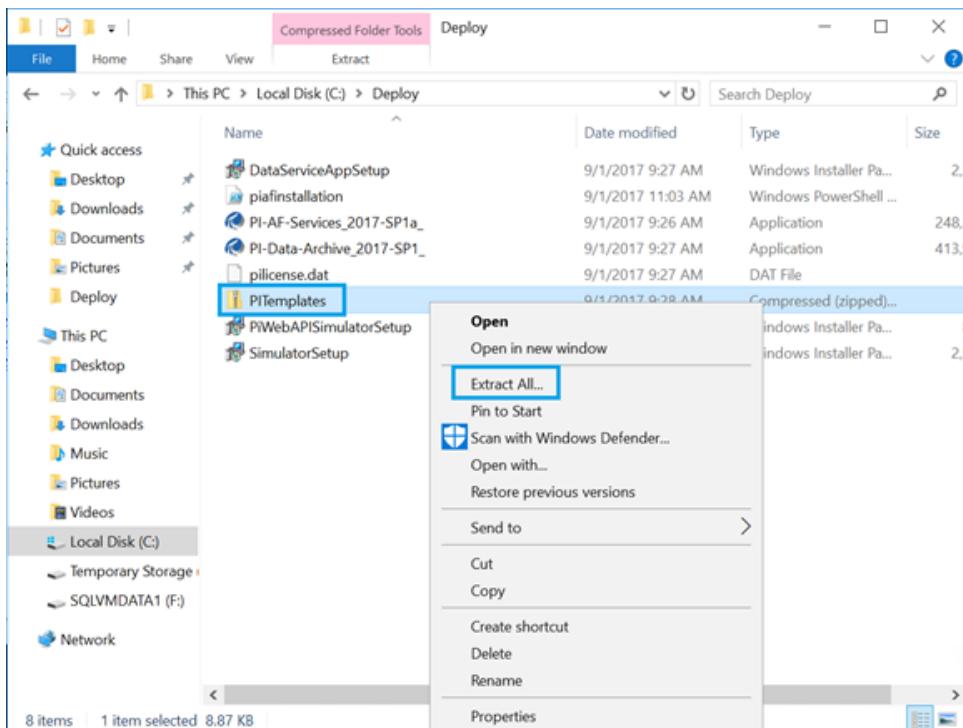


9.6. Import .XML Files into AF Server

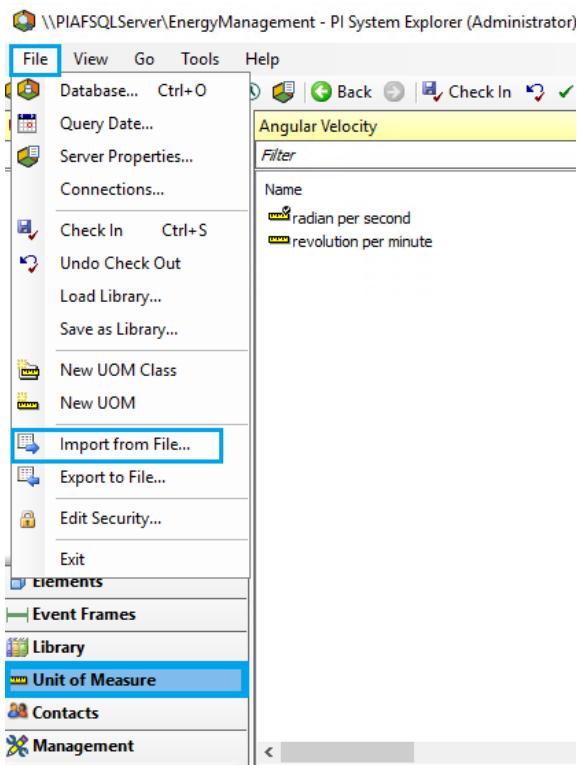
1. From the Bastion host connect to the **PIAFSQLServer** virtual machine through the private address with the credentials provided in the output section.
2. Navigate to **PI System Explorer > Select Database > Click on Energy Management > Click on OK.**



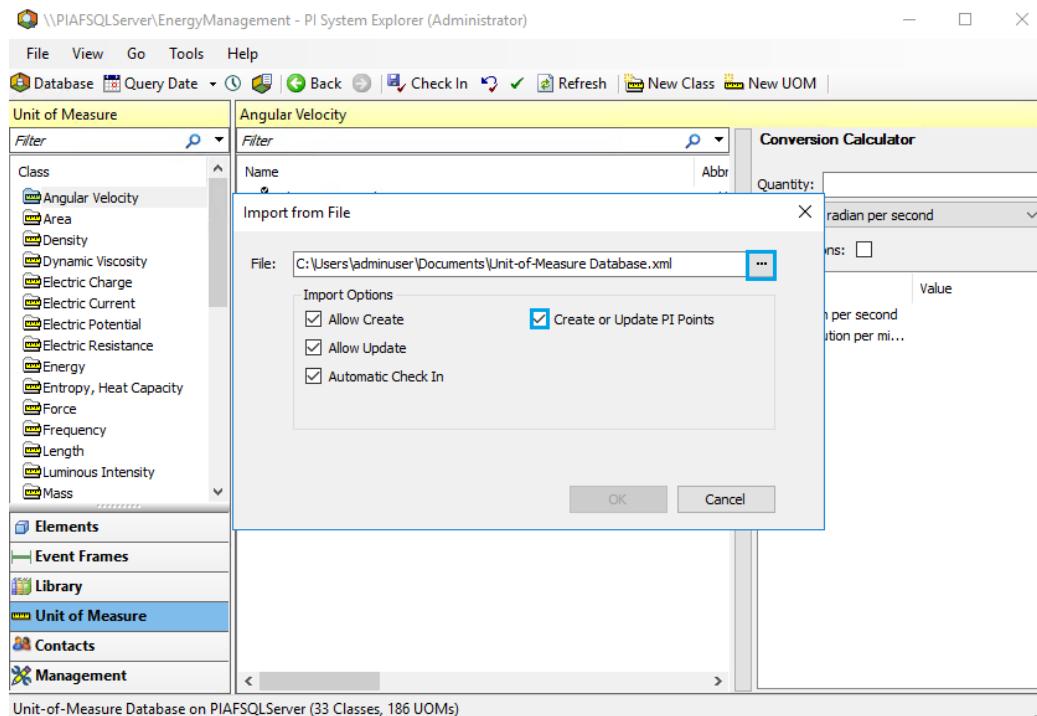
3. Navigate to Local disk (C:) > Deploy > unzip PI templates.



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



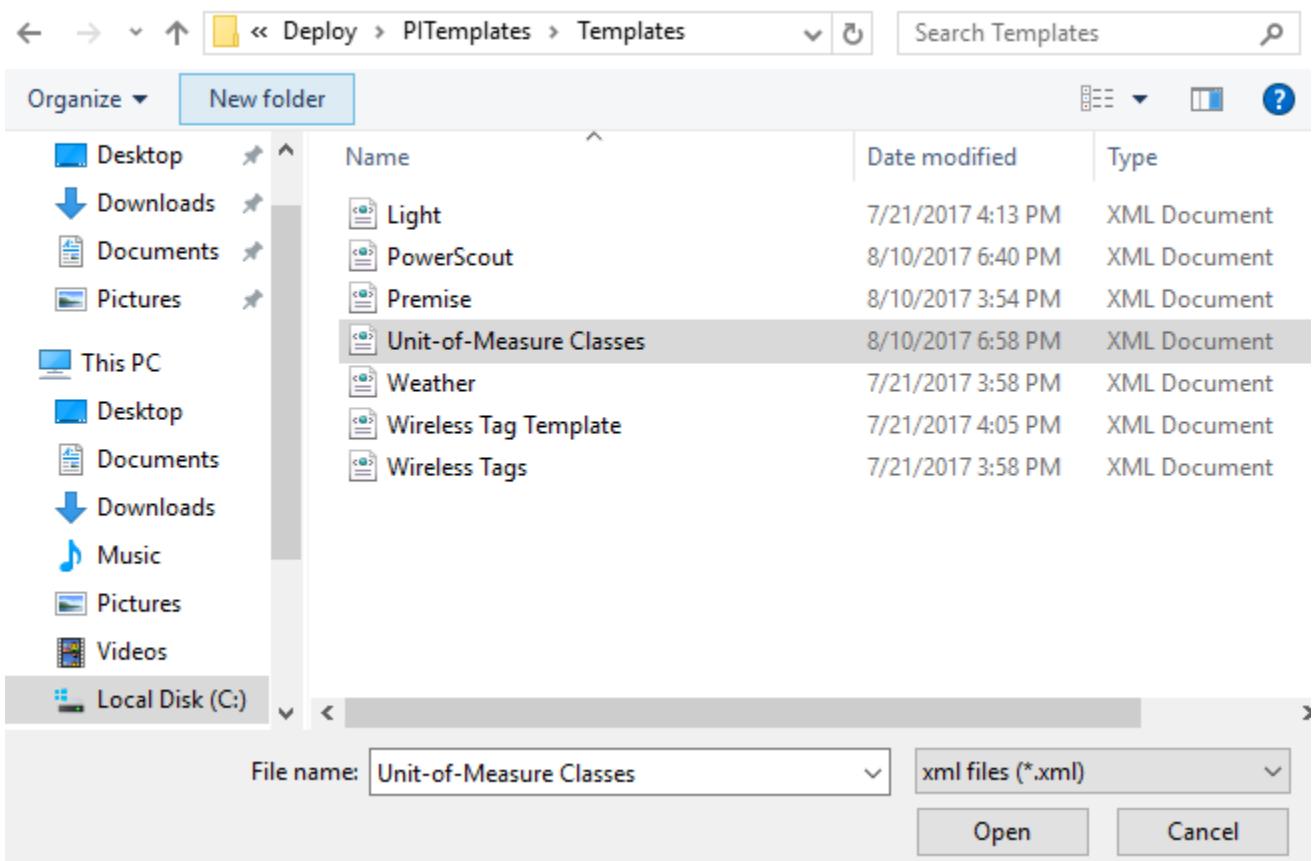
5. Check the box for **Create or Update the PI Points** > browse to **local disk (C:)** > **Deploy > PITemplates** > Select **Unit of Measure Classes** > Click on **Open**.



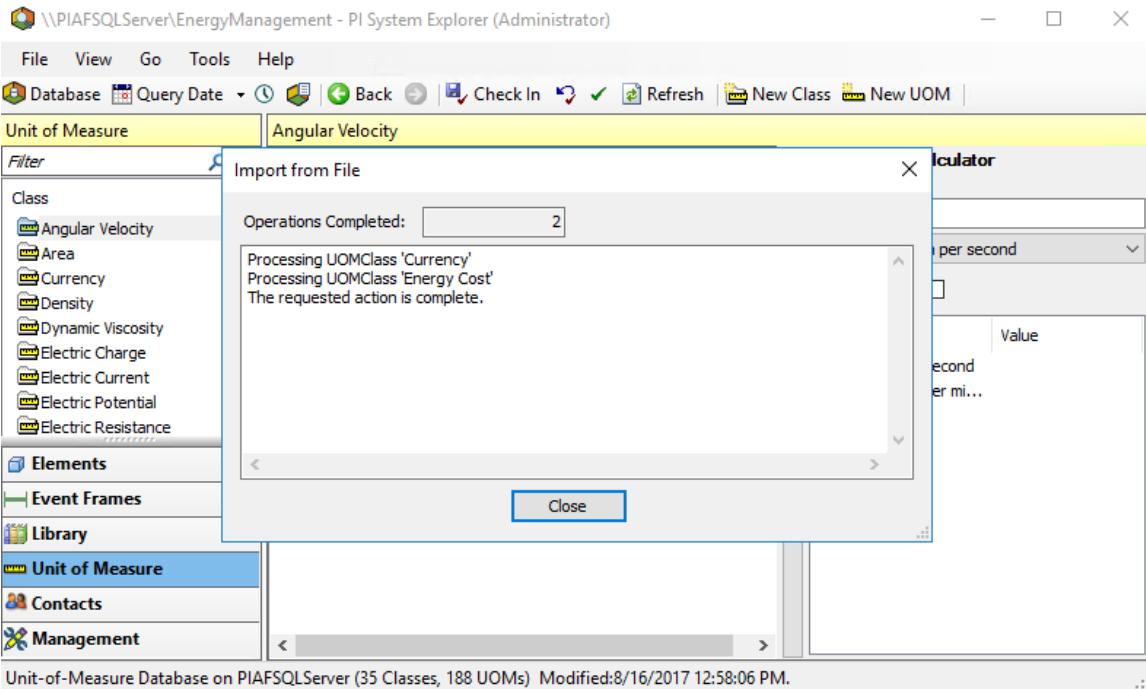
After Open click on ok.

Open

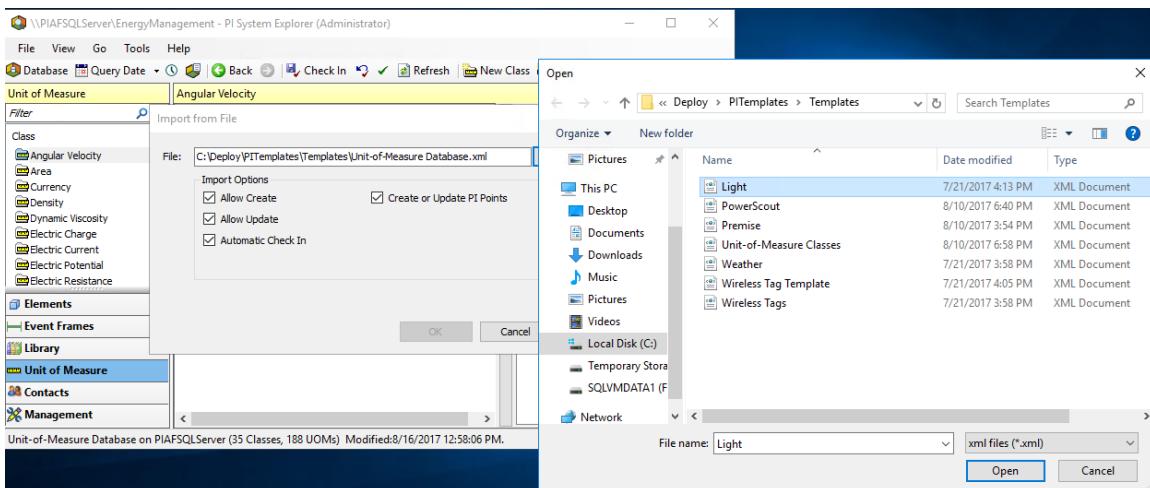
X



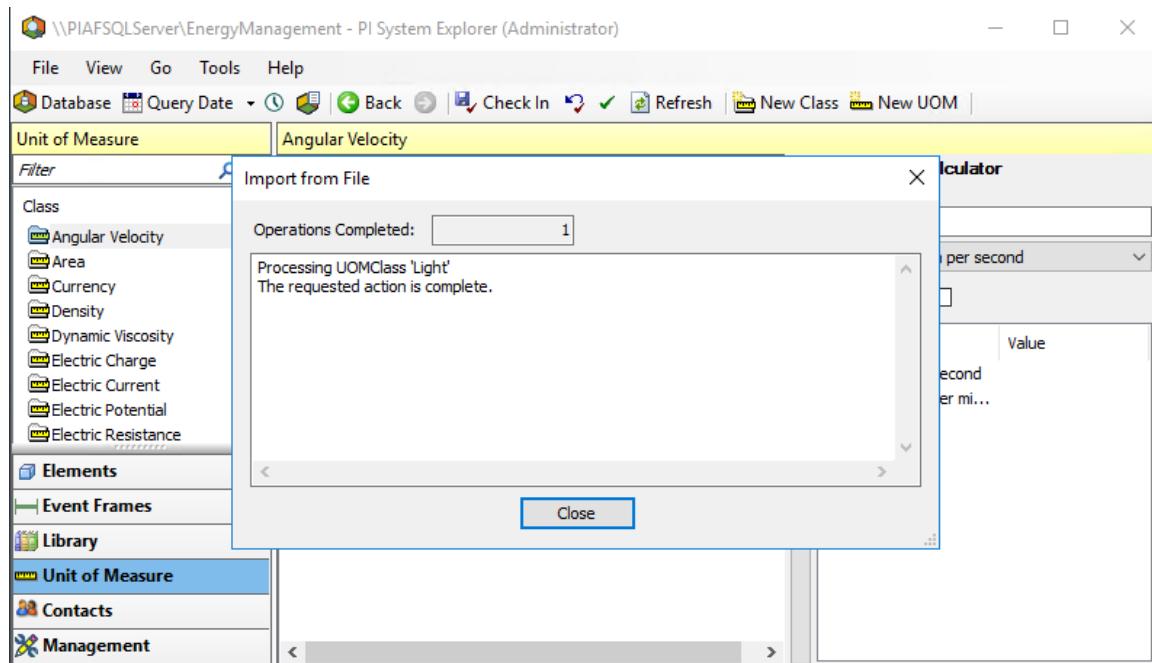
6. You can find the status of the completed operation. Click on **Close**.



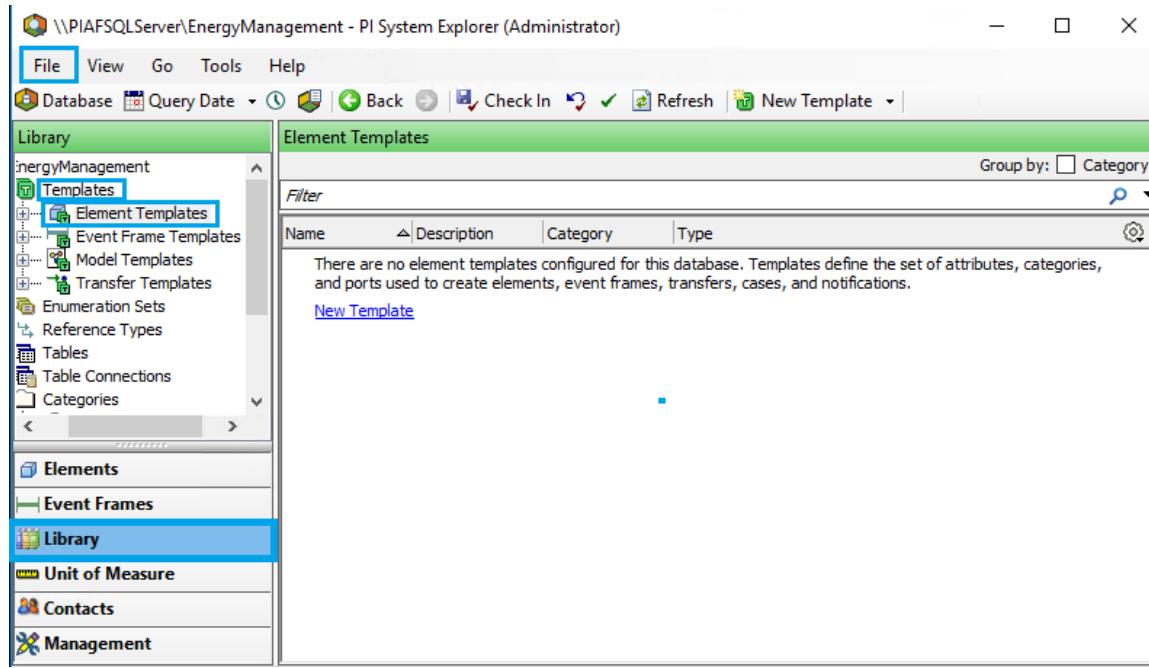
- Again click on the import from file from file menu Check the box **Create or Update the PI Points** > browse to **C:\Deploy\PITemplates** > Select **Light** and click on **Open**.



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



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

Name Description Category Type Template

Name	Description	Category	Type	Template
Premise			None	
Weather			None	
Wireless T...			None	

Group by: Category Template

Search

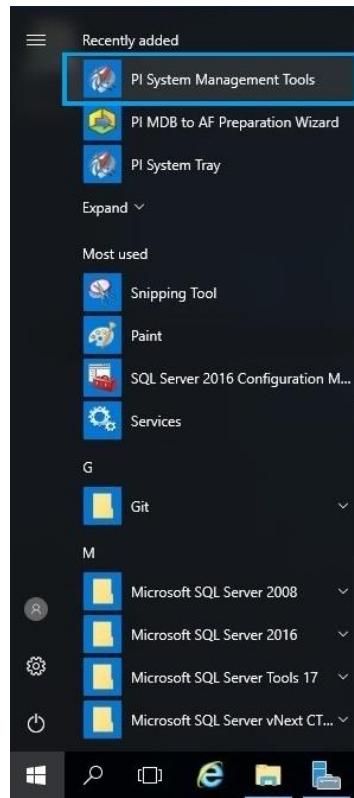
Elements Event Frames Library Unit of Measure Contacts Management

3 Elements

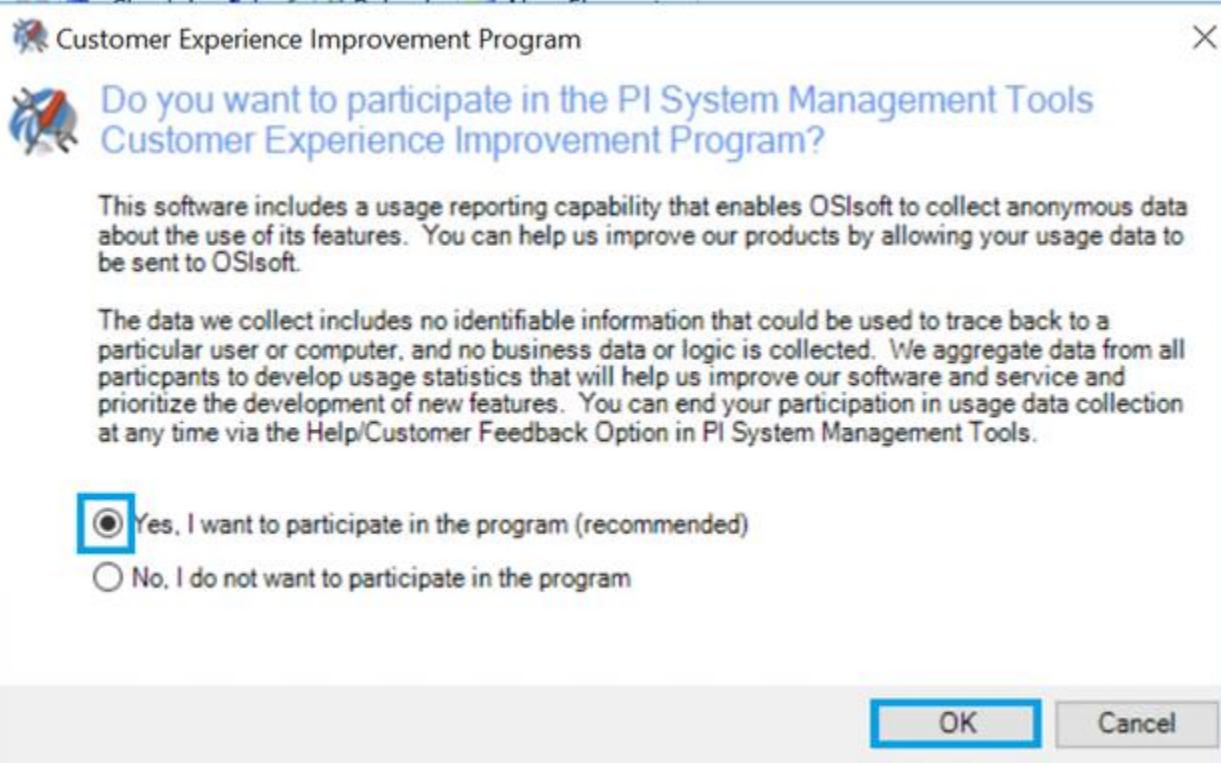
Detailed description: This screenshot shows the PI System Explorer interface. The left sidebar has sections for Elements, Event Frames, Library, Unit of Measure, Contacts, and Management. The main area shows a tree view under 'Elements' with nodes for Premise, Weather, and Wireless Tags. Below this is a table view titled 'Elements' with columns for Name, Description, Category, Type, and Template. Three rows are listed: Premise (Type: None), Weather (Type: None), and Wireless T... (Type: None). The 'Premise' row is currently selected. At the top, there's a navigation bar with tabs for Database, Query Date, Back, Check In, Refresh, and New Element, along with a search bar labeled 'Search Elements'.

9.7. Update Security in PI System Management Tools

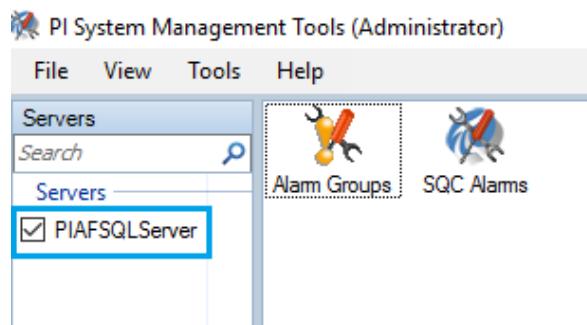
1. From the Start menu, open the **PI System Management Tools**.



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



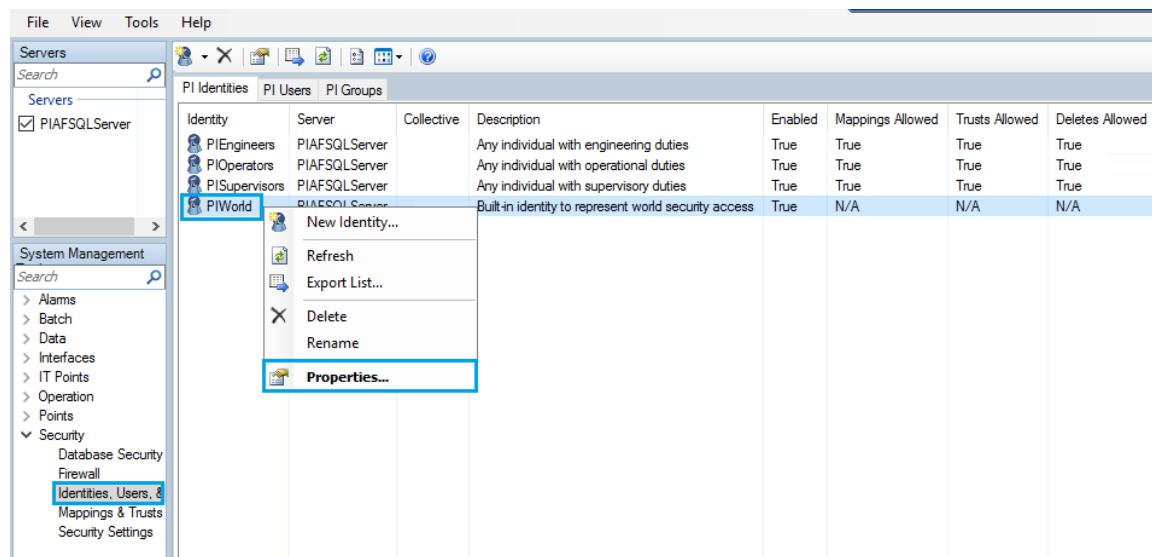
3. Under Servers, check the **PIAFSQLServer** box.



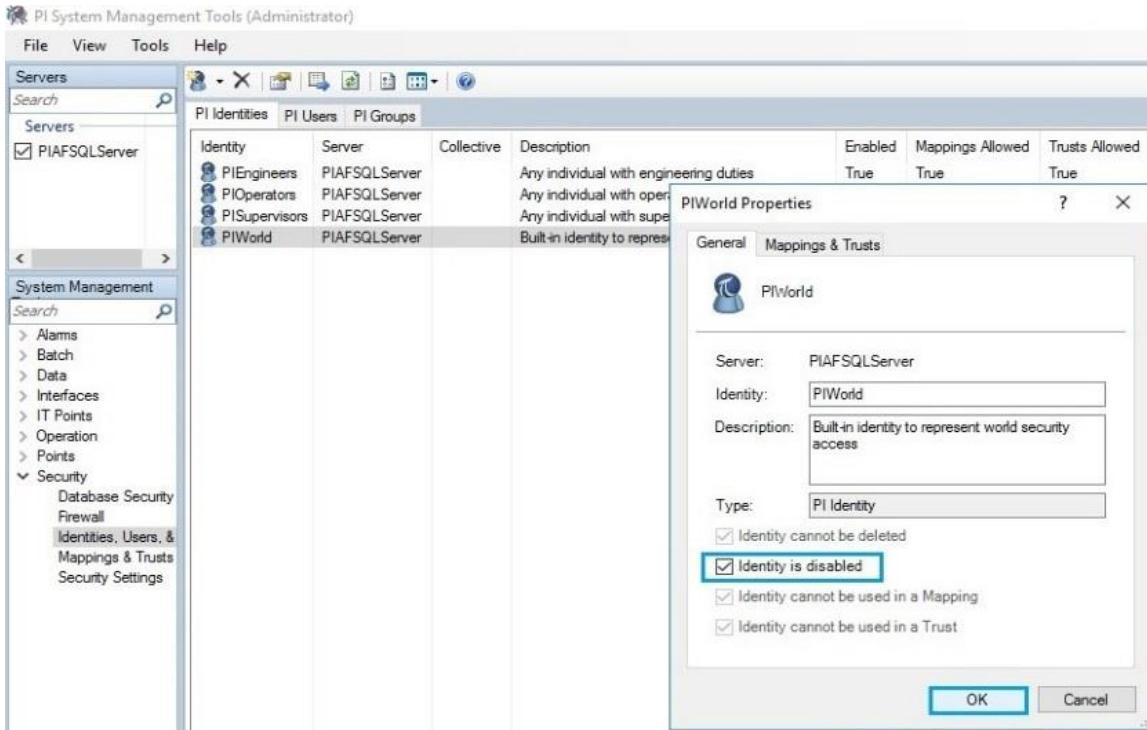
4. Click on **Security** under **System Management**, then click on **Security Settings**.



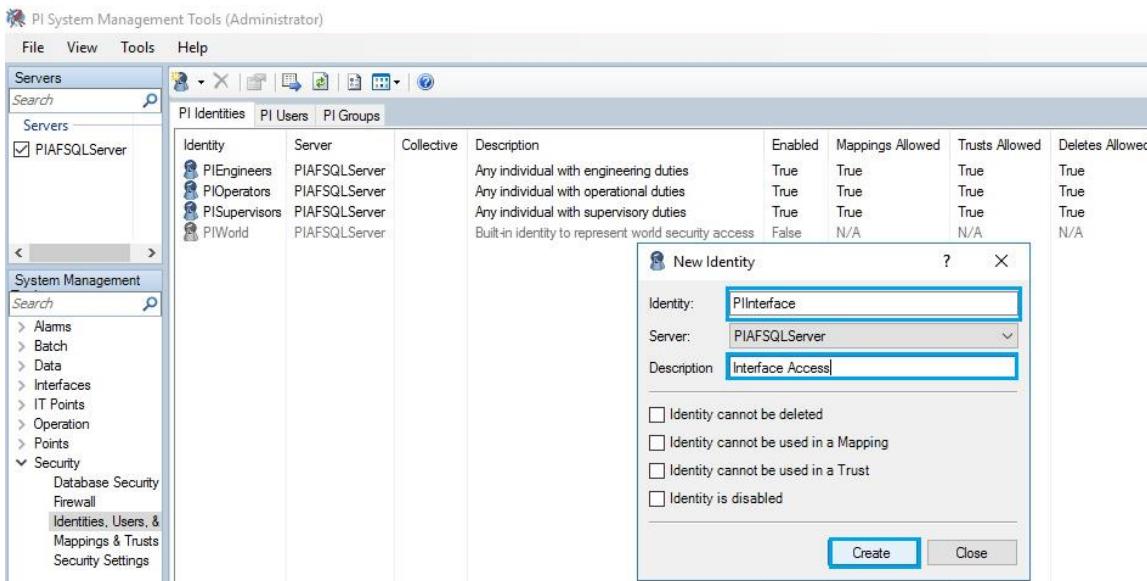
5. Click on **Identities, Users and Groups**, then right-click on **PIWorld** under PI identities and select **Properties**.



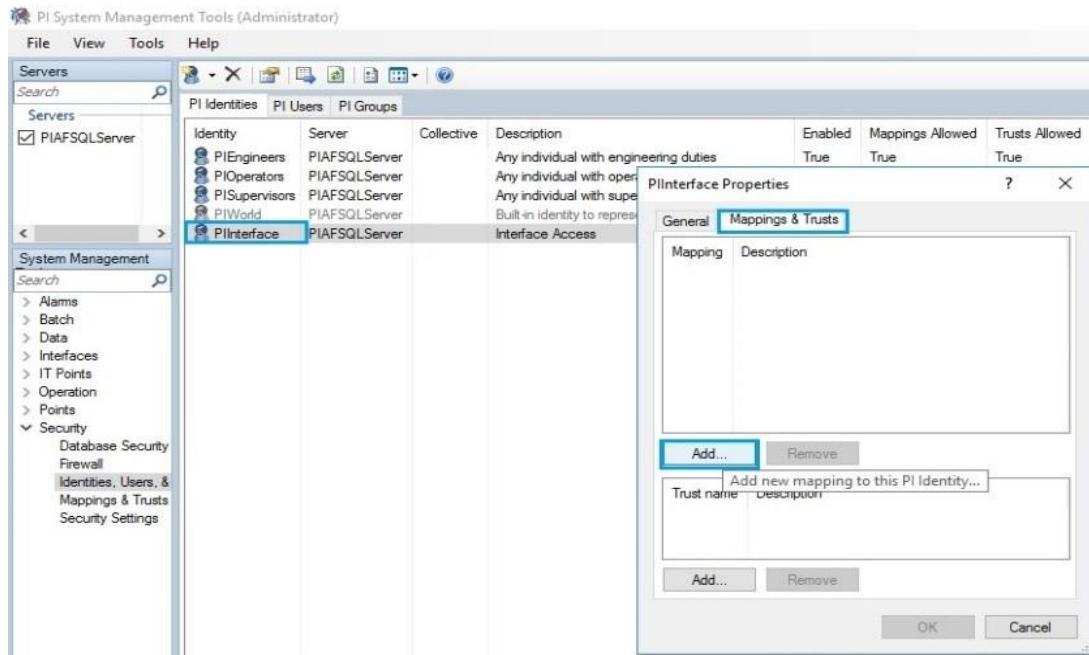
6. Select the **Identity is disabled** checkbox and click on **OK**.



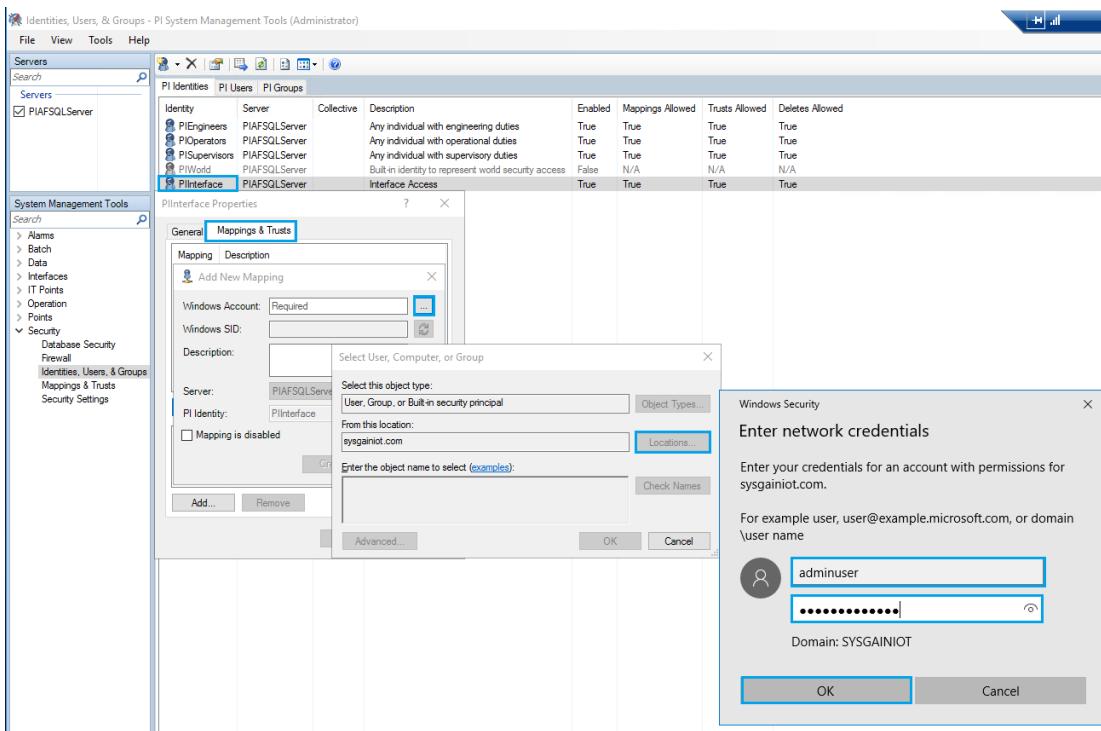
7. The **Enabled** column under **PIWorld** will appear as **False**.
 8. Right-click **PI Identities** to create a new identity. Give the identity the name **PIInterface** and the description **Interface Access**, then click on **Create**.



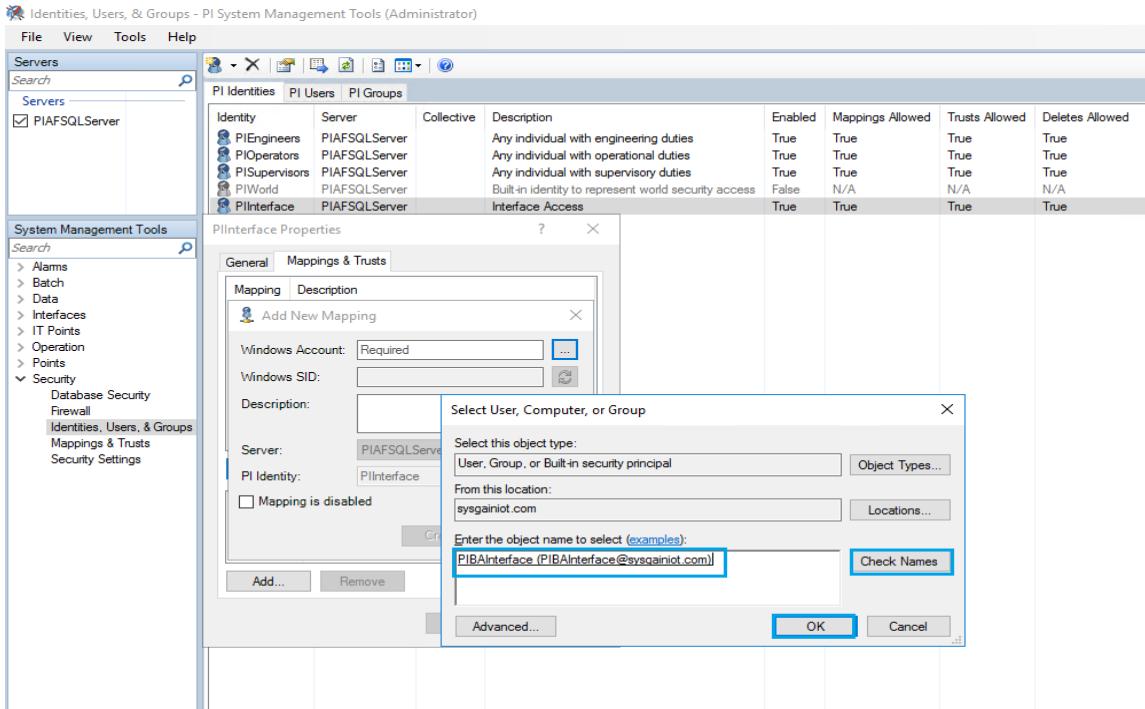
9. Right-click on the newly created **PIInterface** identity, then go to **Properties > Mappings & Trusts**, then click on **Add**.



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.

Servers

Identity	Server	Collective	Description	Enabled	Mappings Allowed	Trusts Allowed	Deletes Allowed
PIEngineers	PIAFSQLServer		Any individual with engineering duties	True	True	True	True
PLOperators	PIAFSQLServer		Any individual with operational duties	True	True	True	True
PISupervisors	PIAFSQLServer		Any individual with supervisory duties	True	True	True	True
PIWorld	PIAFSQLServer		Built-in identity to represent world security access	False	N/A	N/A	N/A
PIInterface	PIAFSQLServer		Interface Access	True	True	True	True

PIInterface Properties

Add New Mapping

Windows Account: SYSGAINIOT\PIBAInterface

Windows SID: S-1-5-21-767990737-295617089-

Description:

Server: PIAFSQLServer

PI Identity: PIInterface

Mapping is disabled

Create

OK Cancel

Add... Remove

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

Servers

Identity	Server	Collective	Description	Enabled	Mappings Allowed	Trusts Allowed	Deletes Allowed
PIEngineers	PIAFSQLServer		Any individual with engineering duties	True	True	True	True
PLOperators	PIAFSQLServer		Any individual with operational duties	True	True	True	True
PISupervisors	PIAFSQLServer		Any individual with supervisory duties	True	True	True	True
PIWorld	PIAFSQLServer		Built-in identity to represent world security access	False	N/A	N/A	N/A
PIInterface	PIAFSQLServer		Interface Access	True	True	True	True

PIInterface Properties

Mappings & Trusts

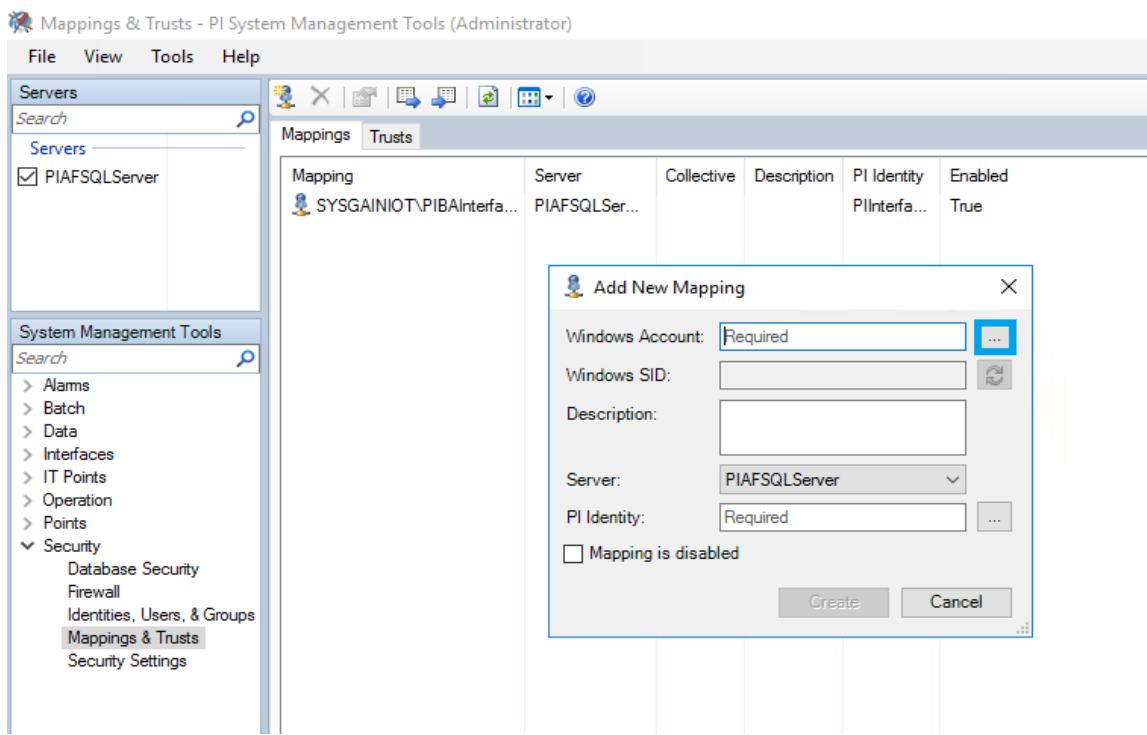
Mapping: SYSGAINIOT\PIBAInterface

Trust name Description

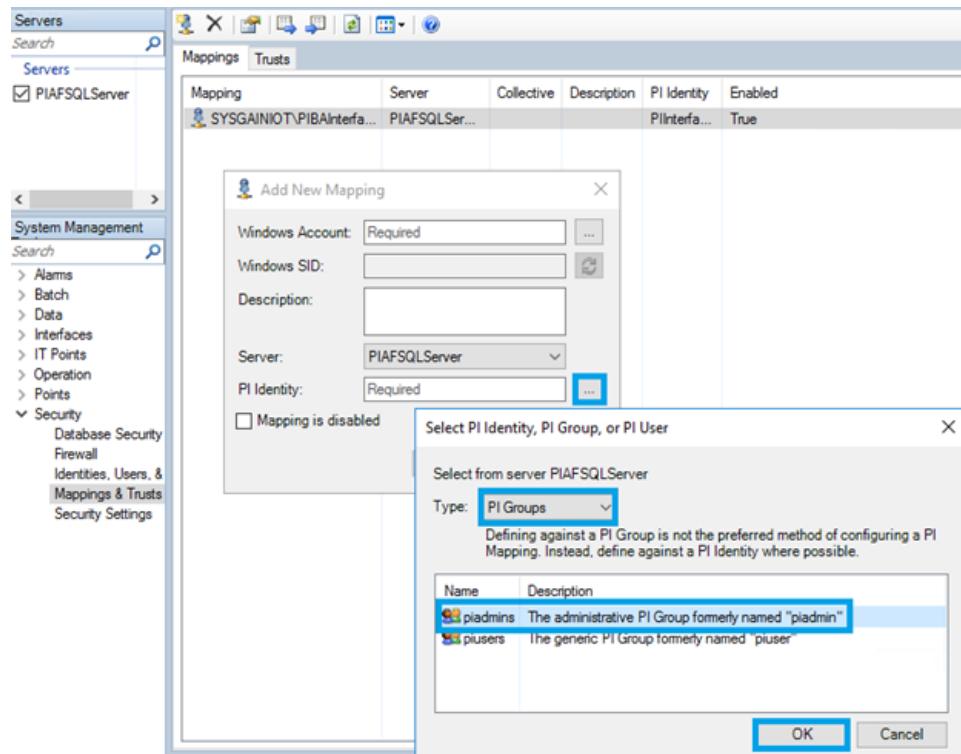
Add... Remove

OK Cancel

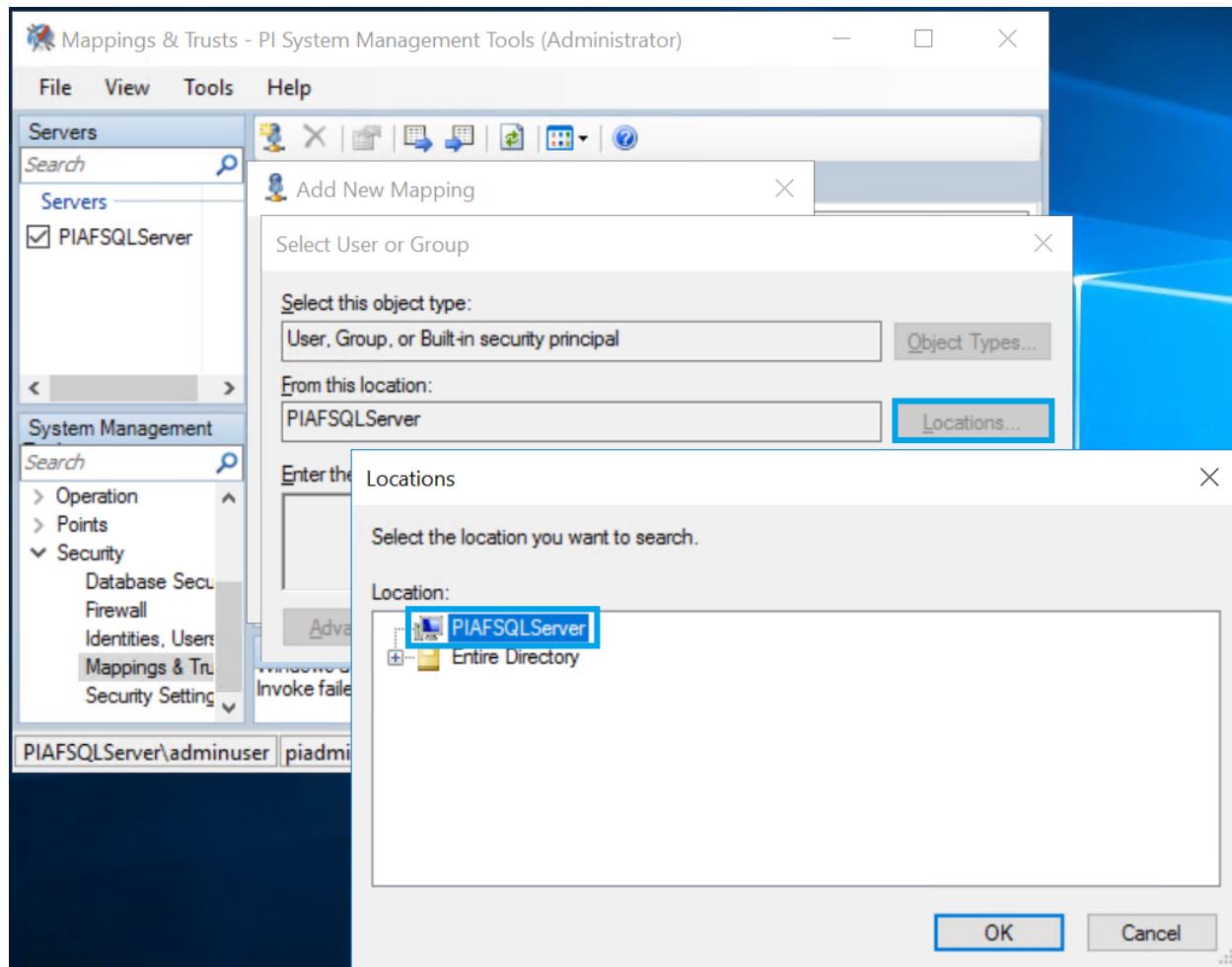
14. Navigate to **Security > Mapping & Trusts** to create a New Mapping. Click on the mappings above symbol to add new mapping.



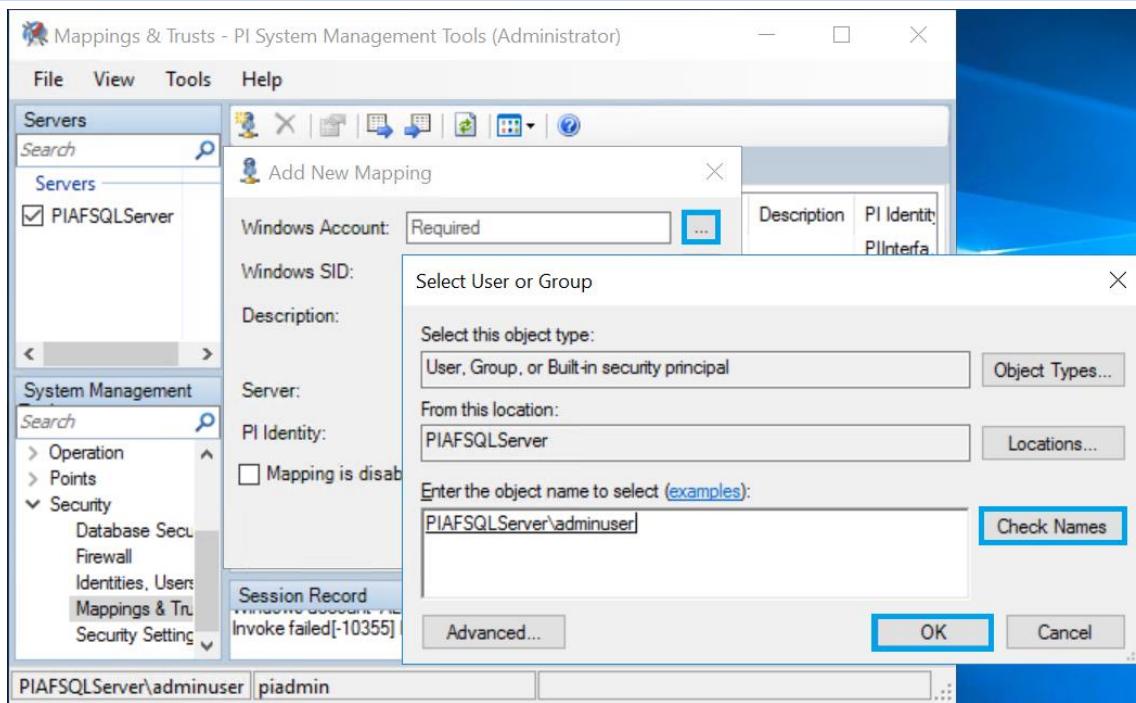
15. Browse the directory in **PI Identity** section, then select **PI groups** under the **Type** dropdown and Select **piadmins** to create PI Identity as **piadmins** click on **OK**.



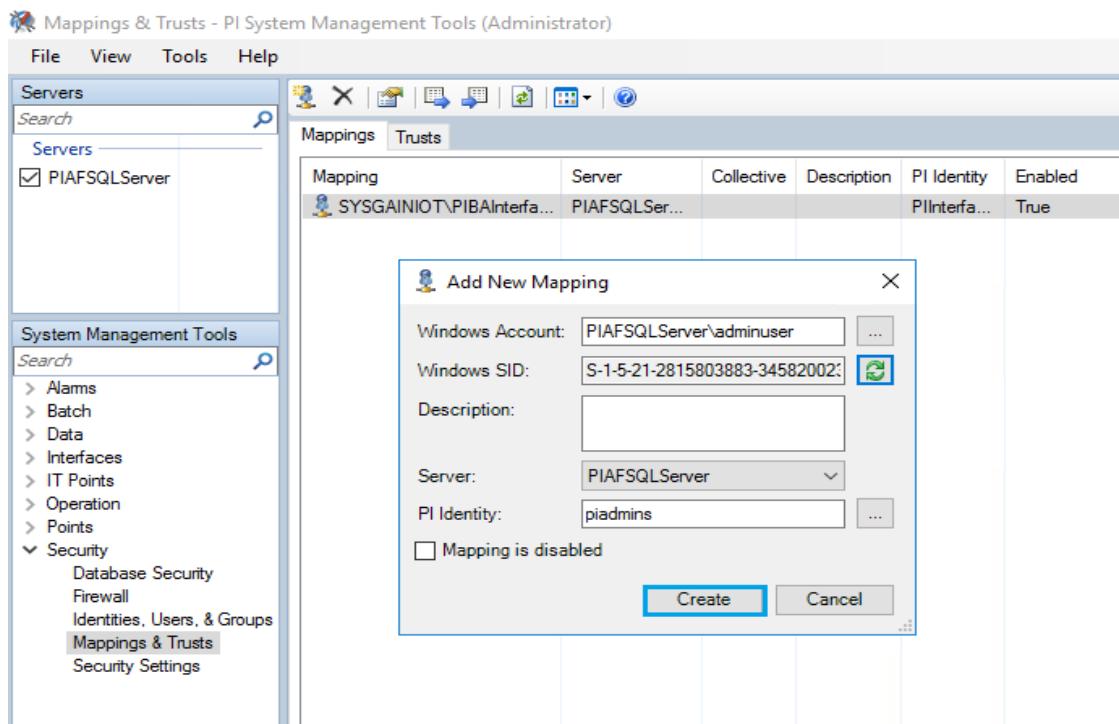
16. Click the dots next to **Windows Account**, then **Locations**, and select the **PIAFSQLServer**.
 Click on **OK**.



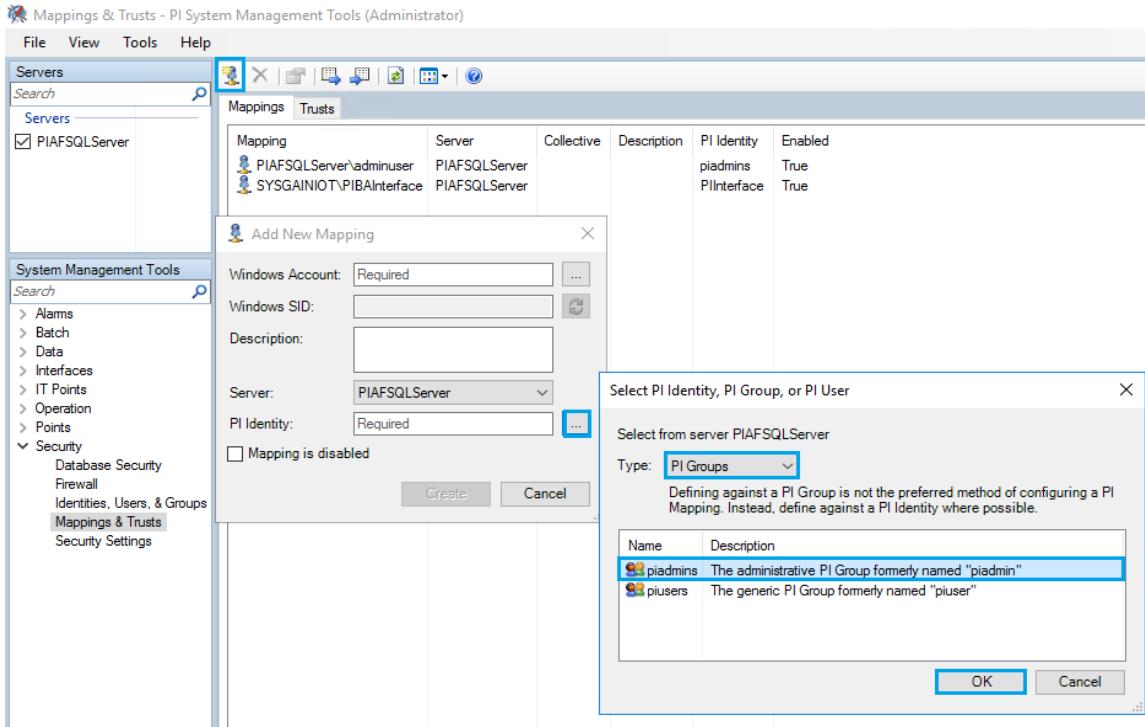
17. Under object name, type adminuser and click on **Check Names**, the following value **PIAFSQLServer\adminuser** will be populated automatically. Click on **OK**.



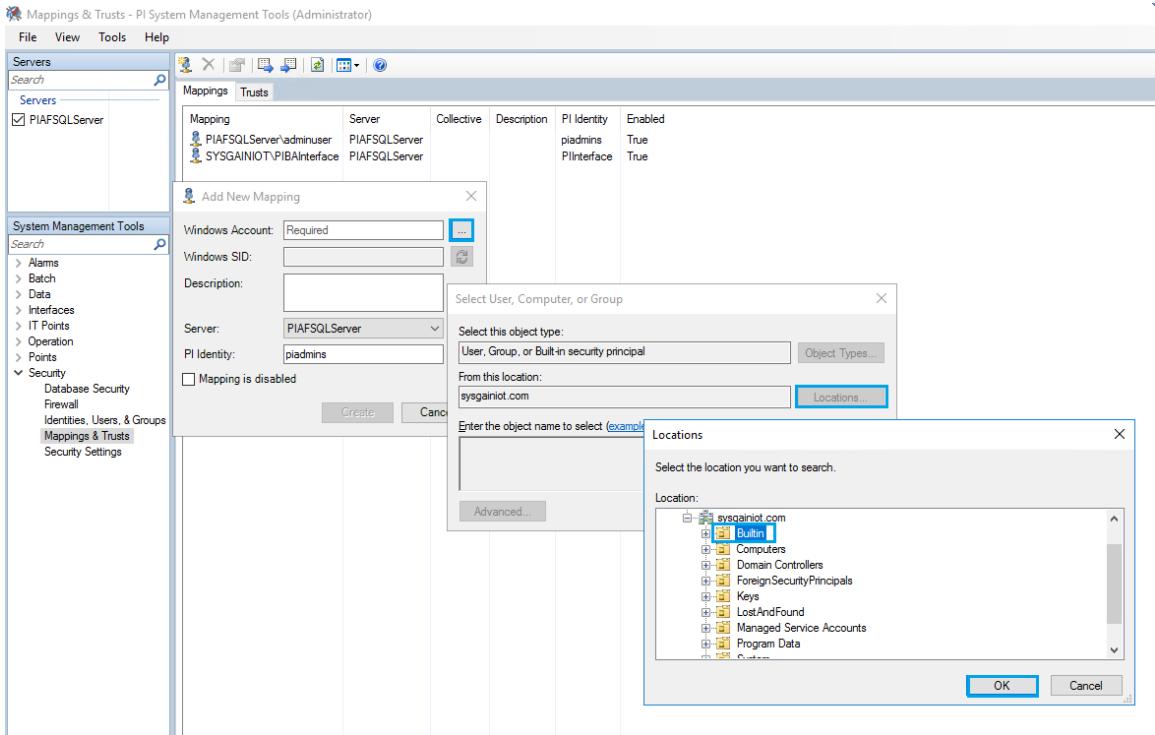
18. Click on **Create**



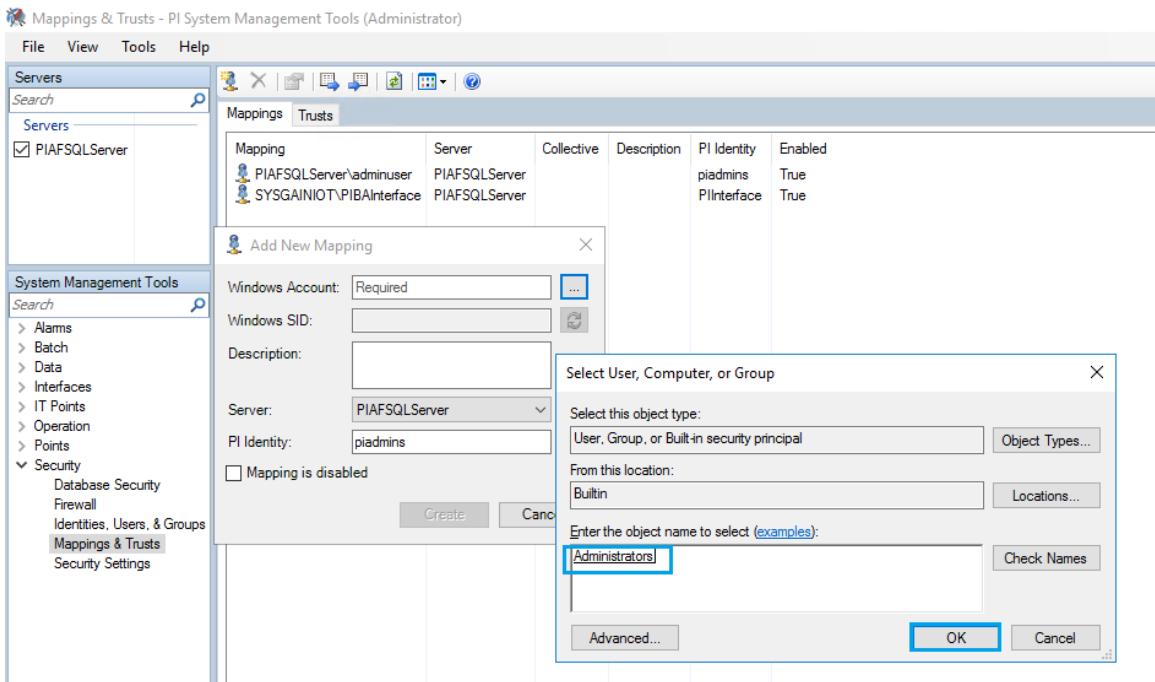
19. Create a new Mapping for **Administrator**. Click on the Mappings above symbol to add new mapping
20. Browse **PI Identity** end, select **Type as PI Groups** > Select **piadmins** > Click on **OK**.



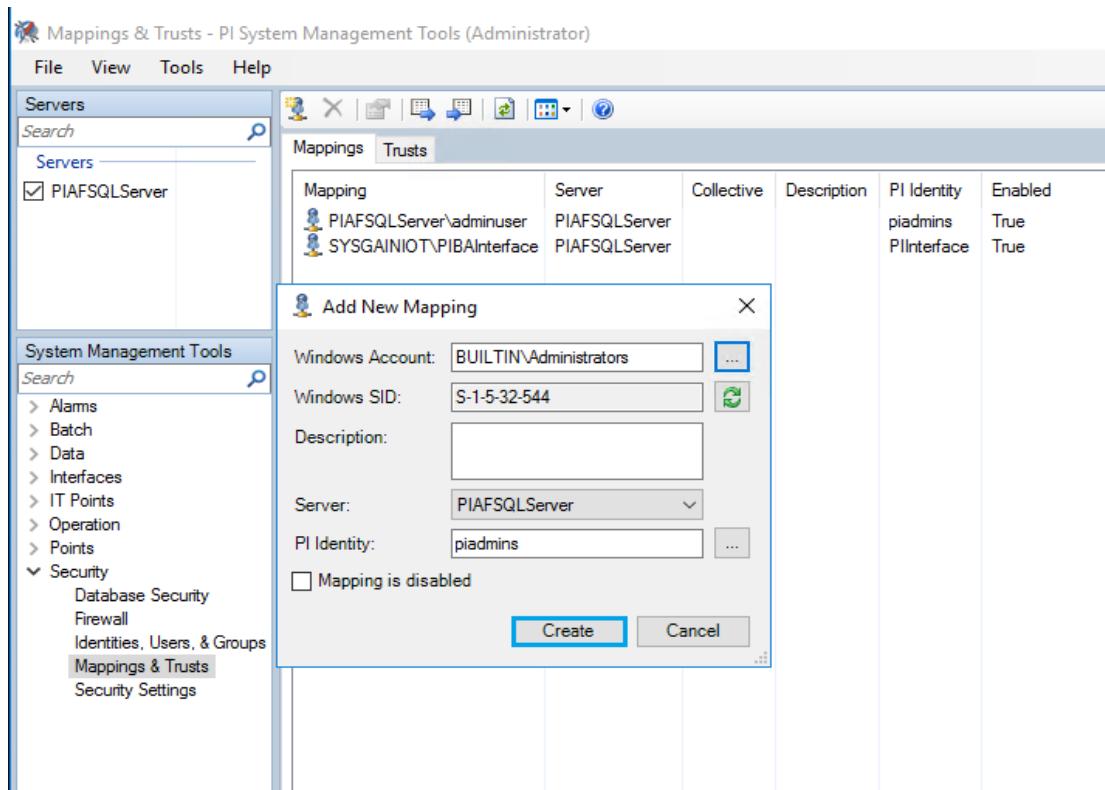
21. Click the Browse dots near **Windows Account** > Select **Locations** > click on **sysgaineriot.com** > Select **Builtin** > Click **OK**.



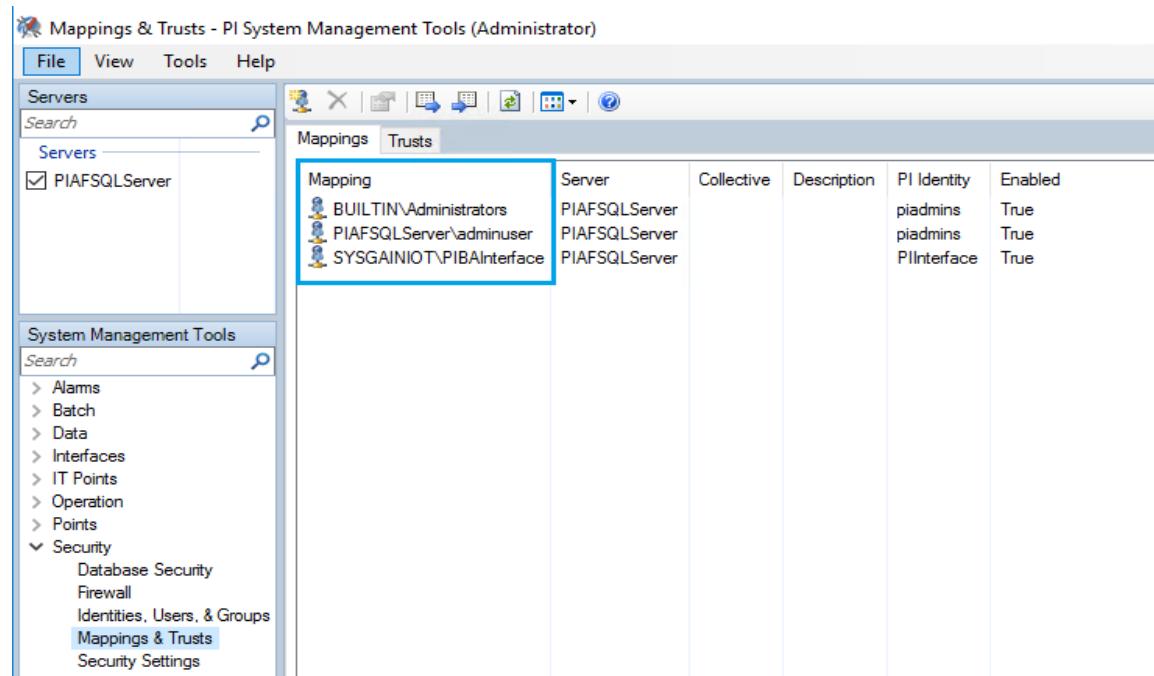
22. Enter the object name as **Administrators**, click on **Check Names** and click on **OK**.



23. Click on **Create**.

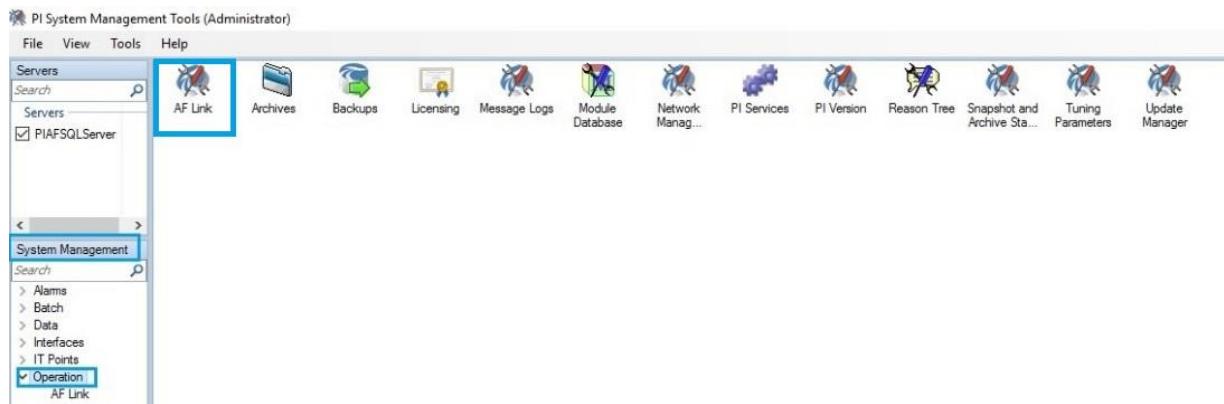


24. Verify the list of Mappings created.

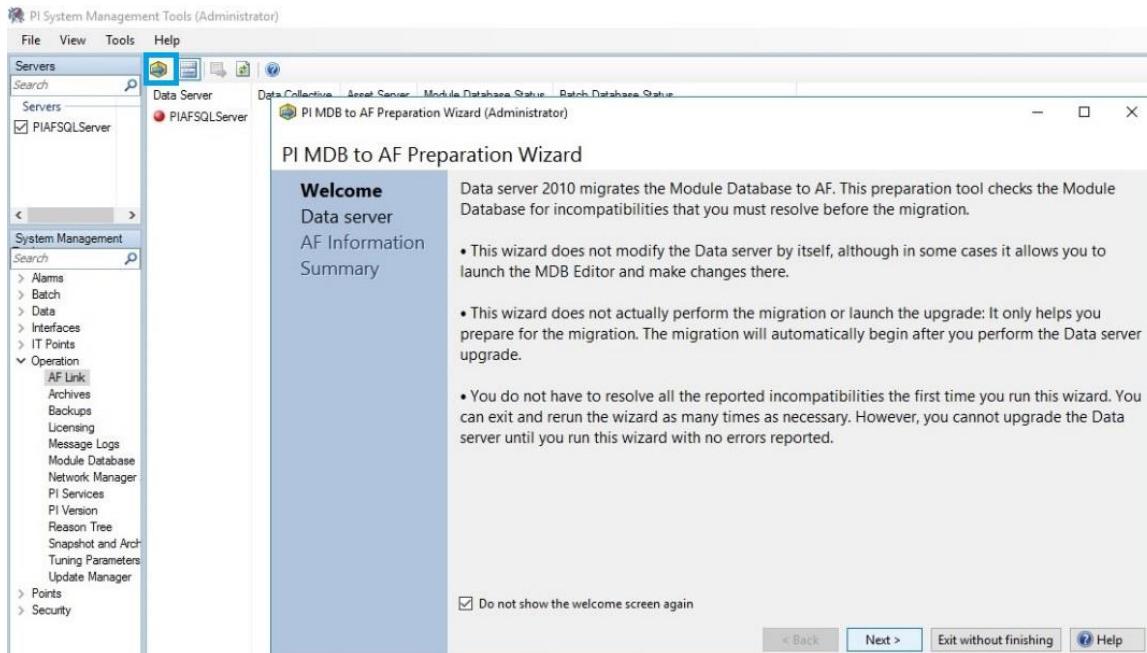


9.8. Prepare Data Server for Module Database(MDB) To Asset Framework(AF)

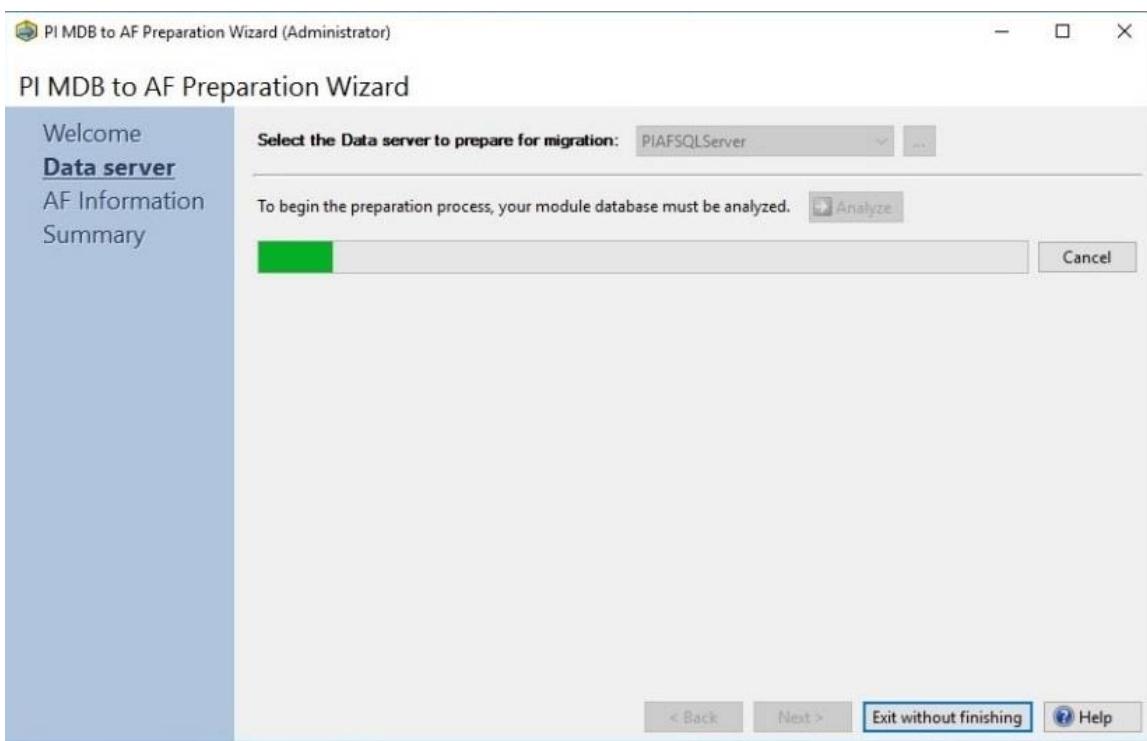
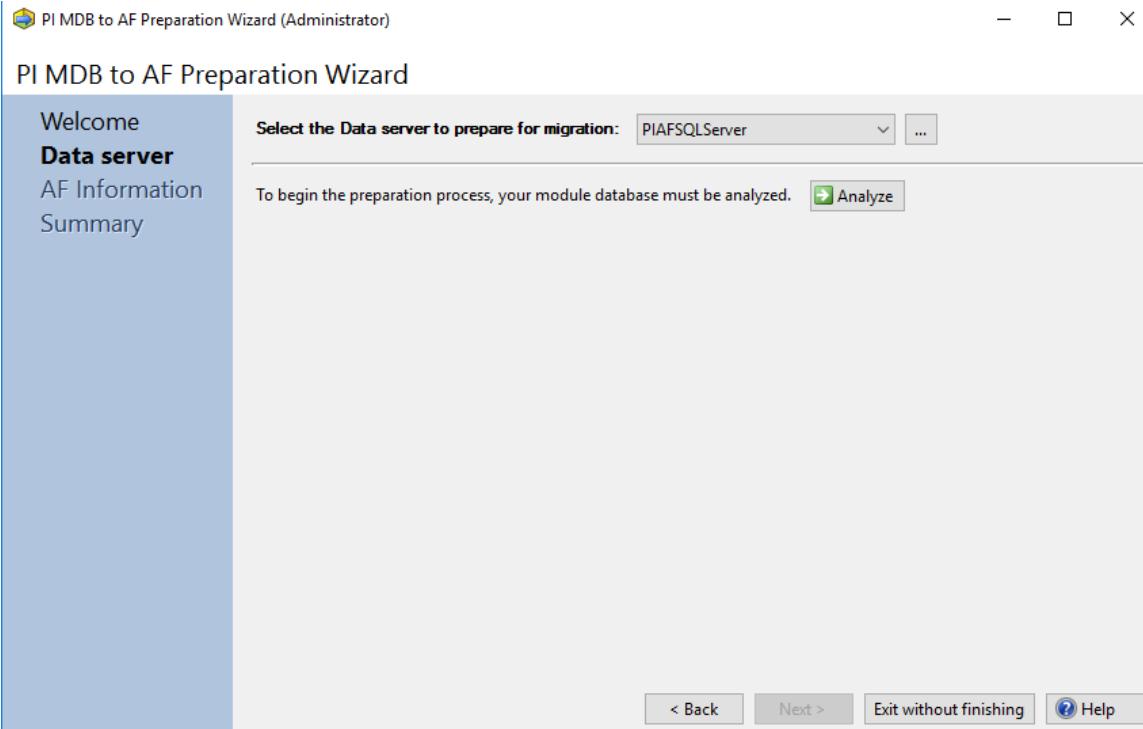
1. Navigate to **PI System Management Tools > Operation > Click on AF link.**



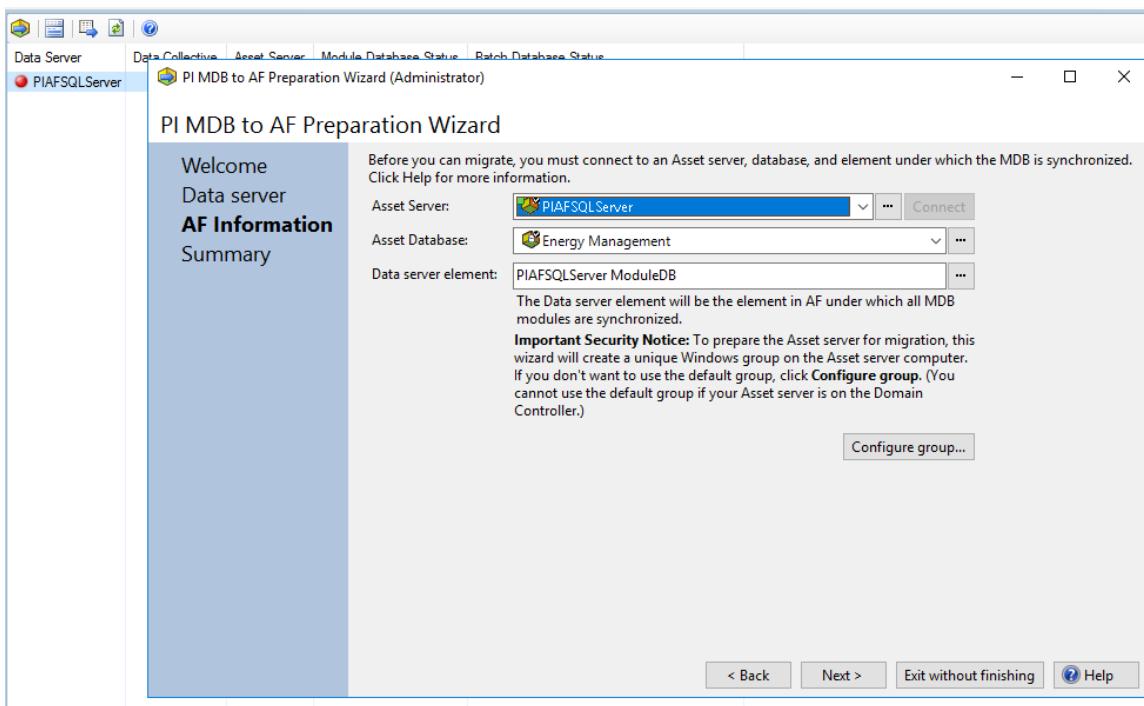
2. Click on **MDB to AF synchronization Wizard** (the symbol just below the **Help** tab). It will open the PI MDB to AF Preparation Wizard as shown below. Tick the do not show the welcome screen again checkbox ,Click on **Next**.



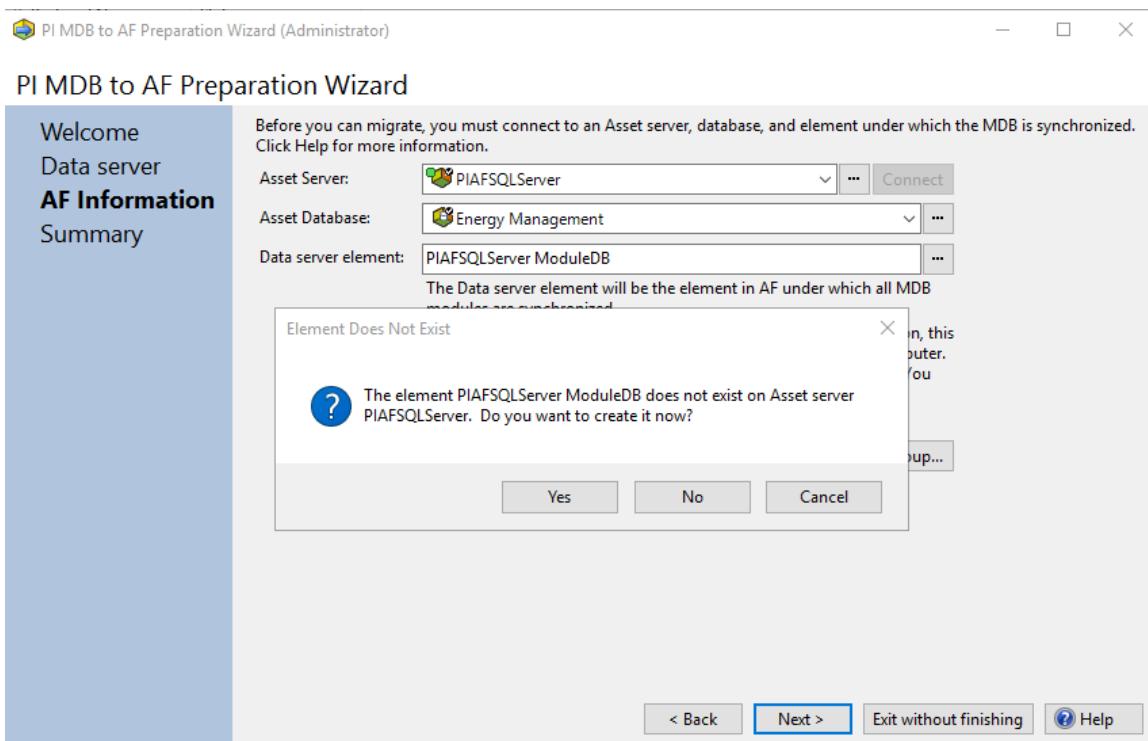
3. Click on **Analyze**, then click on **Next** and again click on **Next** once the process is complete.



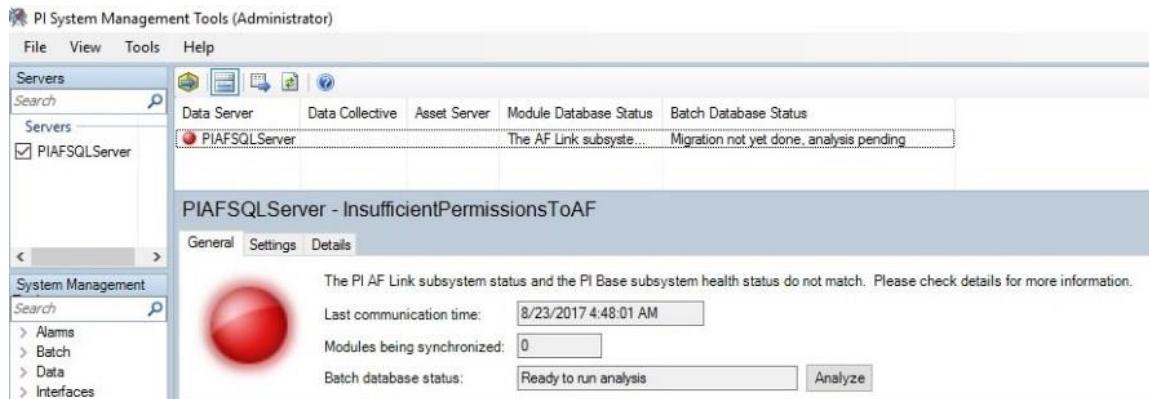
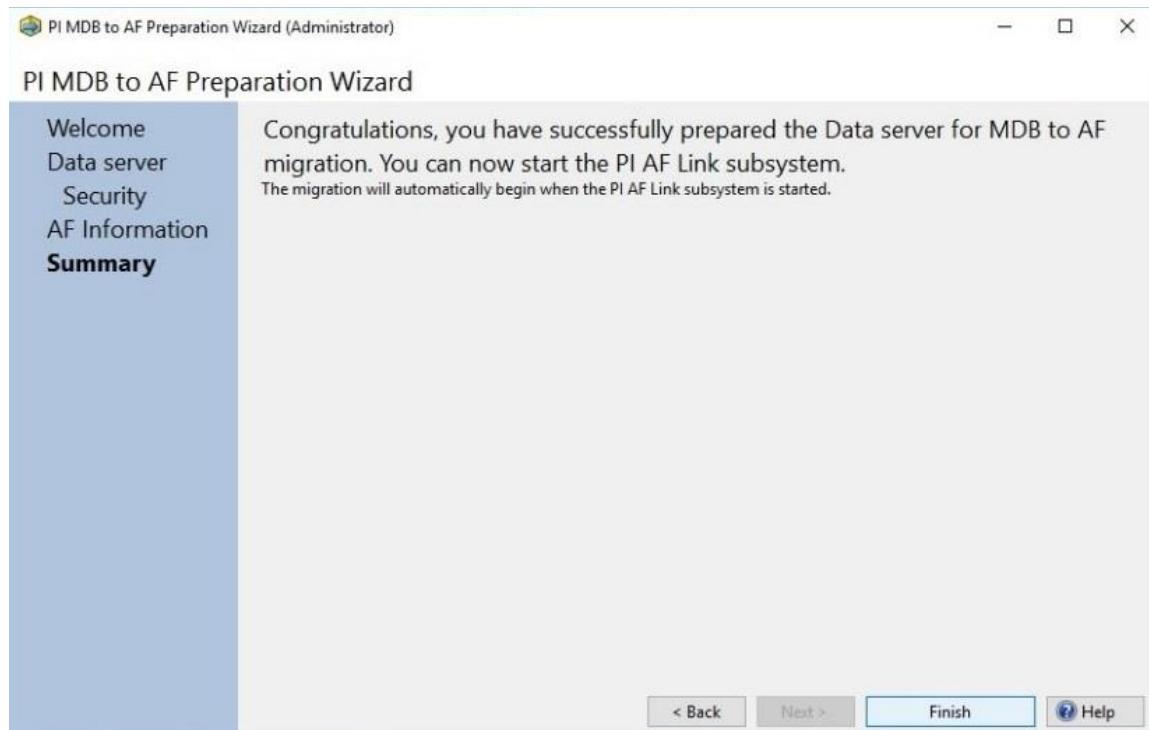
4. In AF Information, set the **Asset Server** as **PIAFS SQLServer**, then click on **Connect**. Set **Asset Database** as **Energy Management**. Click on **Next**.



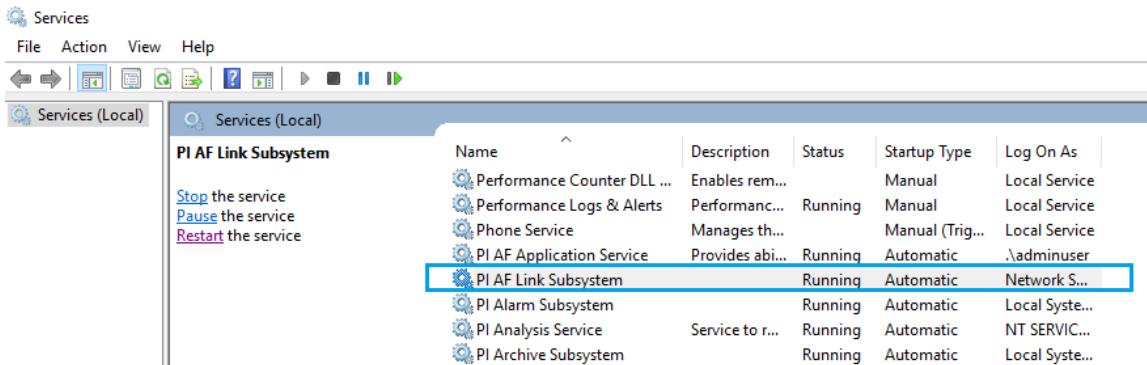
- Click on **Yes** to create a PIAFSQLServer ModuleDB, then click on **Next**.



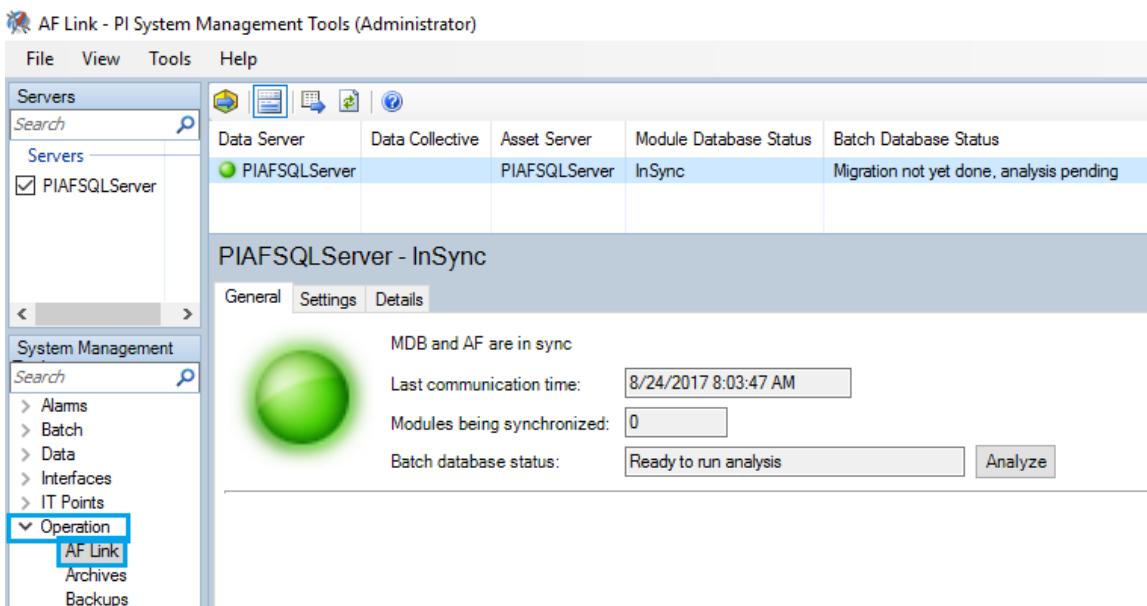
6. Click on **Finish**.



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



- 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

- Open **PI System Explorer** from the Start Menu in the PI System folder.
- 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.

File Search View Go Tools Help

Database Query Date Back Check In Refresh New Element New Attribute

Elements

- Elements
 - Premise
 - Building 1
 - P371602028
 - P371602030
 - Building 2
 - P371602018
 - P371602020
 - Weather
 - Wireless Tags
 - Element Searches

P371602028

General Child Elements Attributes Ports Analyses Notification Rules Version

Filter

Name	Value
Amps L1	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L2	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L3	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps System Avg	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Breaker Details	New (2018) 4th floor panel - almost empty
Breaker Label	PP14 - 5th Fl Electrical Rm
Building	Building 1
Daily Electric Cost	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Daily kWh System	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW L1	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW L2	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW L3	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW System	PI Data Archive 'DESKTOP-J9V7ITT' was not found

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 " \ "

\\PIAFSQLServer\EnergyManagement - PI System Explorer (Administrator)

File Search View Go Tools Help

Database Query Date Back Check In Refresh New Element New Attribute

Search Elements

Elements

- Elements
 - PIAFSQLServer ModuleDB
 - Premise
 - Building 1
 - P371602028
 - P371602030
 - Building 2
 - Weather
 - Wireless Tags
 - Element Searches
- Elements
- Event Frames
- Library
- Unit of Measure
- Contacts
- Management

P371602028

General Child Elements Attributes Ports Analyses Notification Rules Version

Filter

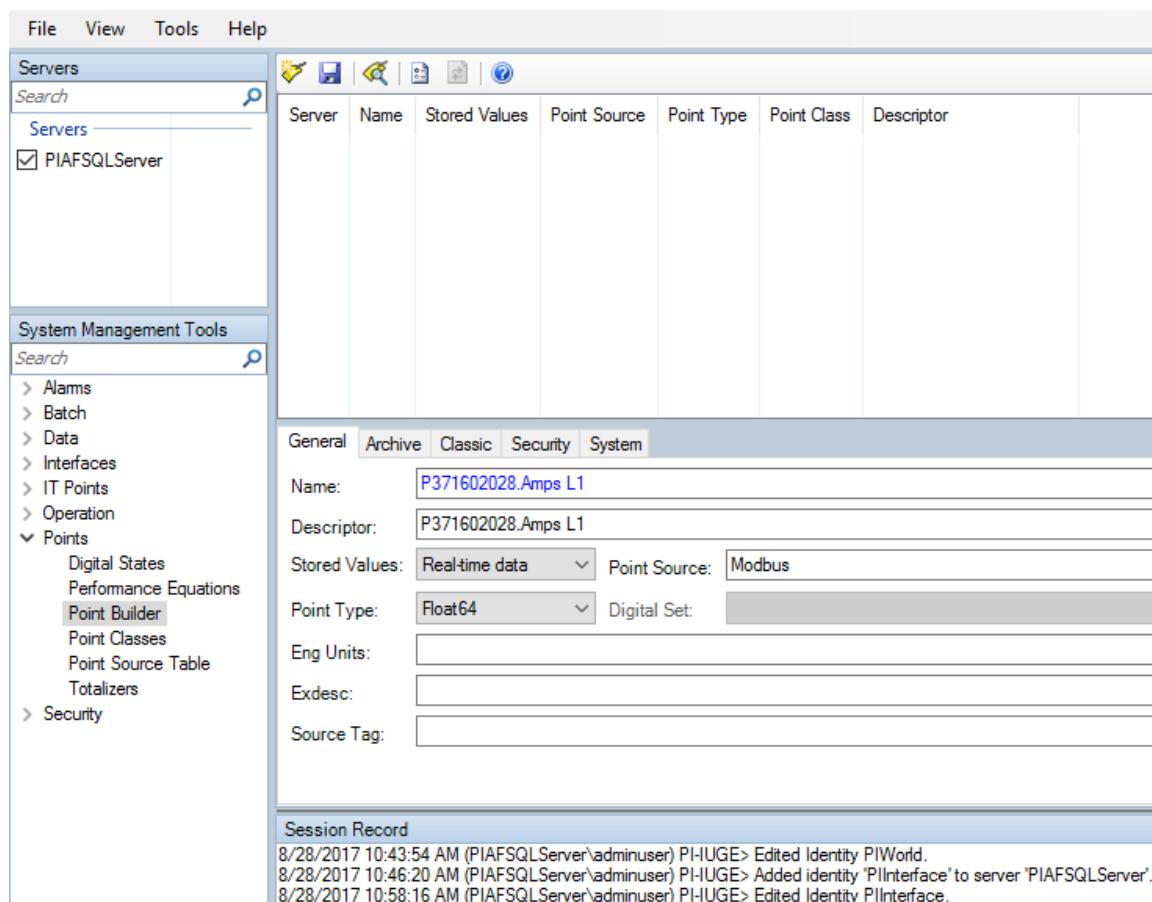
Name	Value
Amps L1	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L2	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L3	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps System Avg	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Breaker Details	New (2018) 4th floor panel - almost empty
Breaker Label	PP14 - 5th Fl Electrical Rm
Building	Building 1
Daily Electric Cost	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Daily kWh System	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW L1	PI Data Archive 'DESKTOP-J9V7ITT' was not found
kW L2	PI Data Archive 'DESKTOP-J9V7ITT' was not found

Settings...

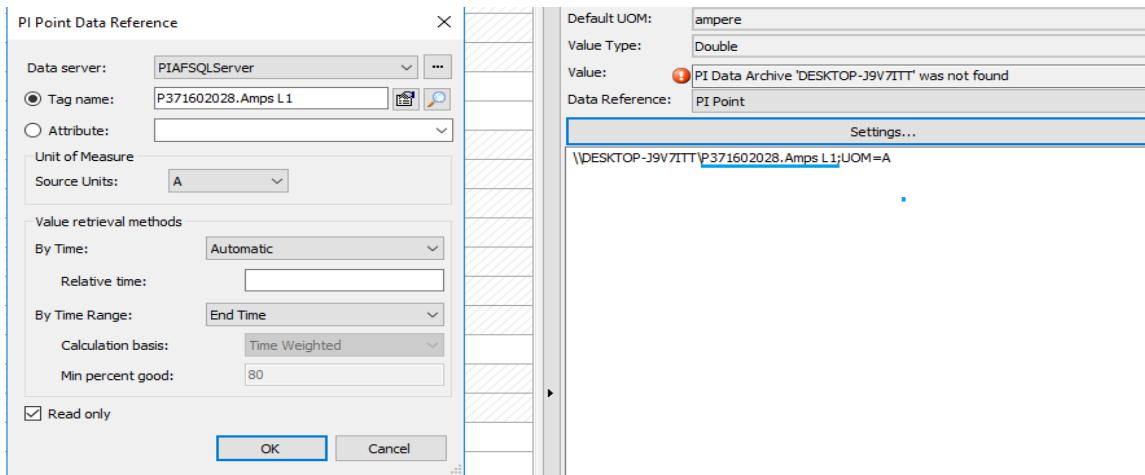
Name: Amps L1
 Description: Individual Phase Currents (A)
 Properties: <None>
 Categories: Current
 Default UOM: ampere
 Value Type: Double
 Value: PI Data Archive 'DESKTOP-J9V7ITT' was not found
 Data Reference: PI Point
 Settings...
 \\DESKTOP-J9V7ITT\P371602028.Amps L1;UOM=A

Limits Forecasts

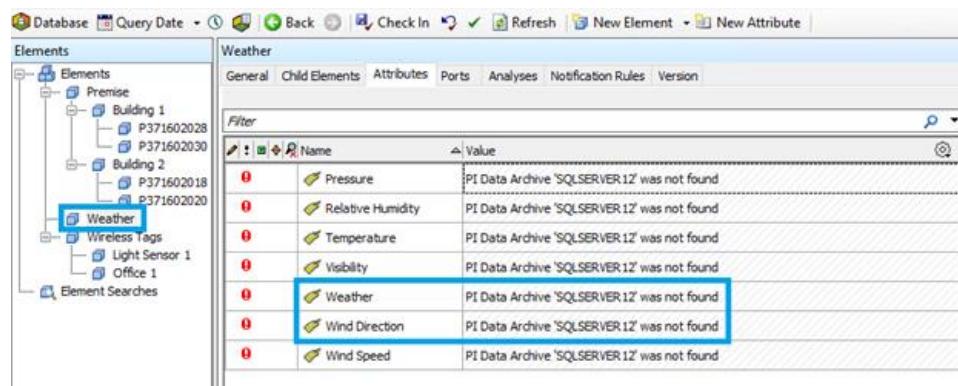
4. Open **PI System Management Tools** from the Start Menu in the PI System folder, then navigate to **Points > Point Builder**.
5. Paste the PI point content copied from PI explorer in the **Name** and **Descriptor** fields.
Enter **Point Source** as “**Modbus**”, then **Point type** as **Float 64**.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



Name	Value
Pressure	PI Data Archive 'SQLSERVER.12' was not found
Relative Humidity	PI Data Archive 'SQLSERVER.12' was not found
Temperature	PI Data Archive 'SQLSERVER.12' was not found
Visibility	PI Data Archive 'SQLSERVER.12' was not found
Weather	PI Data Archive 'SQLSERVER.12' was not found
Wind Direction	PI Data Archive 'SQLSERVER.12' was not found
Wind Speed	PI Data Archive 'SQLSERVER.12' was not found

Servers

Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor
PIAFSQLServer	P371602028.Amps L1	Real-time data	Modbus	Float64	classic	P371602028.Amps L1
	P371602028.Amps L2	Real-time data	Modbus	Float64	classic	P371602028.Amps L2
	P371602028.Amps L3	Real-time data	Modbus	Float64	classic	P371602028.Amps L3
	P371602028.Amps System Avg	Real-time data	Modbus	Float64	classic	P371602028.Amps System Avg
	P371602028.Daily Electric Cost.60e6094f-e554-5e8f-1742-54def61fbe81	Real-time data	Modbus	Float64	classic	P371602028.Daily Electric Cost
	P371602028.Daily kWh System.3b67c63a-d3c7-5b43-1d5b-4d7994c899bc	Real-time data	Modbus	Float64	classic	P371602028.Daily kWh System
	P371602028.kW L1	Real-time data	Modbus	Float64	classic	P371602028.kW L1
	P371602028.kW L2	Real-time data	Modbus	Float64	classic	P371602028.kW L2
	P371602028.kW L3	Real-time data	Modbus	Float64	classic	P371602028.kW L3
	P371602028.kW System	Real-time data	Modbus	Float64	classic	P371602028.kW System
	P371602028.Monthly_Electric Cost.4b4292a6-69ff-517c-7ec95-10a07794d1604	Real-time data	Modbus	Float64	classic	P371602028.Monthly_Electric Cost

System Management Tools

General Archive Classic Security System

Name: NWS_KFNL_WindDirection

Descriptor: NWS_KFNL_WindDirection

Stored Values: Real-time data Point Source: Modbus

Point Type: String Digital Set:

Eng Units:

Exdesc:

Source Tag:

Session Record

```
8/28/2017 12:32:04 PM (PIAFSQLServer\administrator) PI-PB> Successfully created point P371602030.Volts L2 to Neutral on server PIAFSQLServer.
8/28/2017 12:32:19 PM (PIAFSQLServer\administrator) PI-PB> Successfully created point P371602030.Volts L3 to Neutral on server PIAFSQLServer.
8/28/2017 12:34:22 PM (PIAFSQLServer\administrator) PI-PB> Successfully created point P371602018.Amps L1 on server PIAFSQLServer.
8/28/2017 12:34:39 PM (PIAFSQLServer\administrator) PI-PB> Successfully created point P371602018.Amps L2 on server PIAFSQLServer.
```

9.10. Install and Run The Piweb Simulator Setup

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

 Home

Some settings are managed by your organization.

Find a setting 

Time & language

Date and time

 Date & time

9:35 AM, Thursday, August 24, 2017

Set time automatically

 On

Set time zone automatically

 OffChange date and time
(UTC-08:00) Baja California

(UTC-08:00) Coordinated Universal Time-08

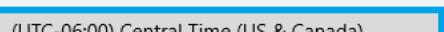
(UTC-08:00) Pacific Time (US & Canada)

(UTC-07:00) Arizona

(UTC-07:00) Chihuahua, La Paz, Mazatlan

(UTC-07:00) Mountain Time (US & Canada)

(UTC-06:00) Central America

(UTC-06:00) Central Time (US & Canada)

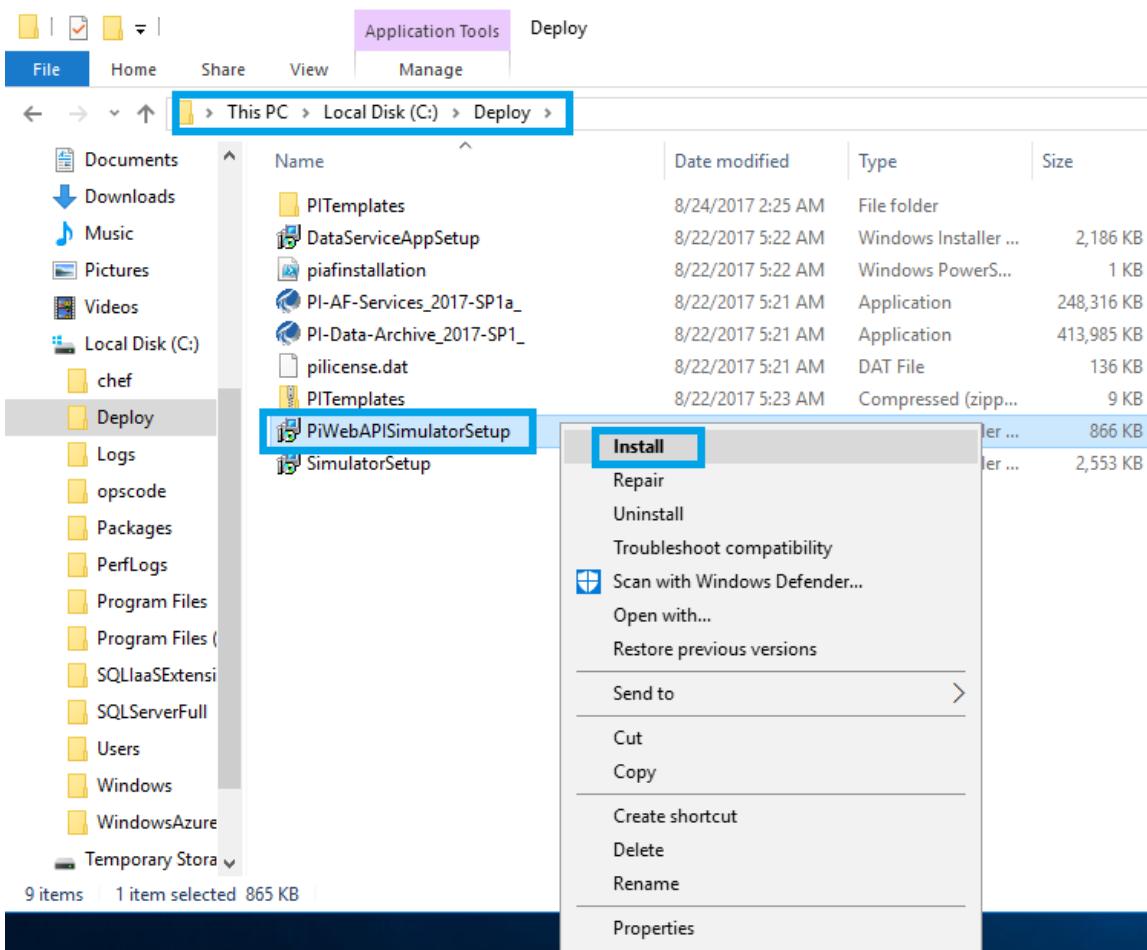
(UTC-06:00) Easter Island

(UTC-06:00) Guadalajara, Mexico City, Monterrey

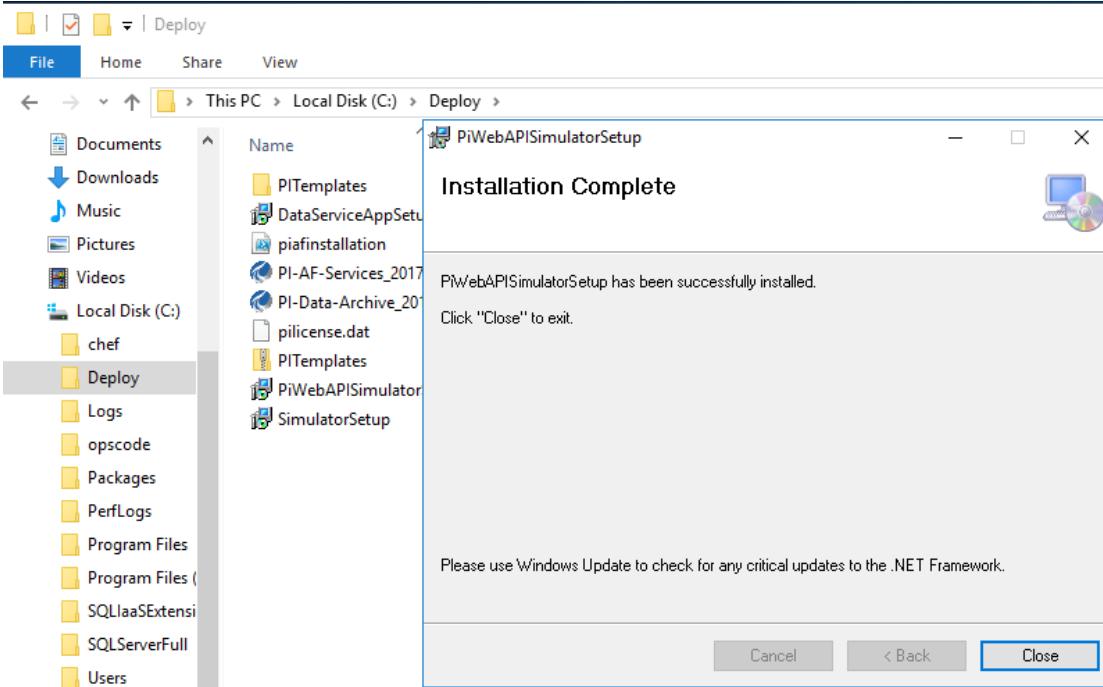
First day of week: Sunday

Short date: 8/24/2017

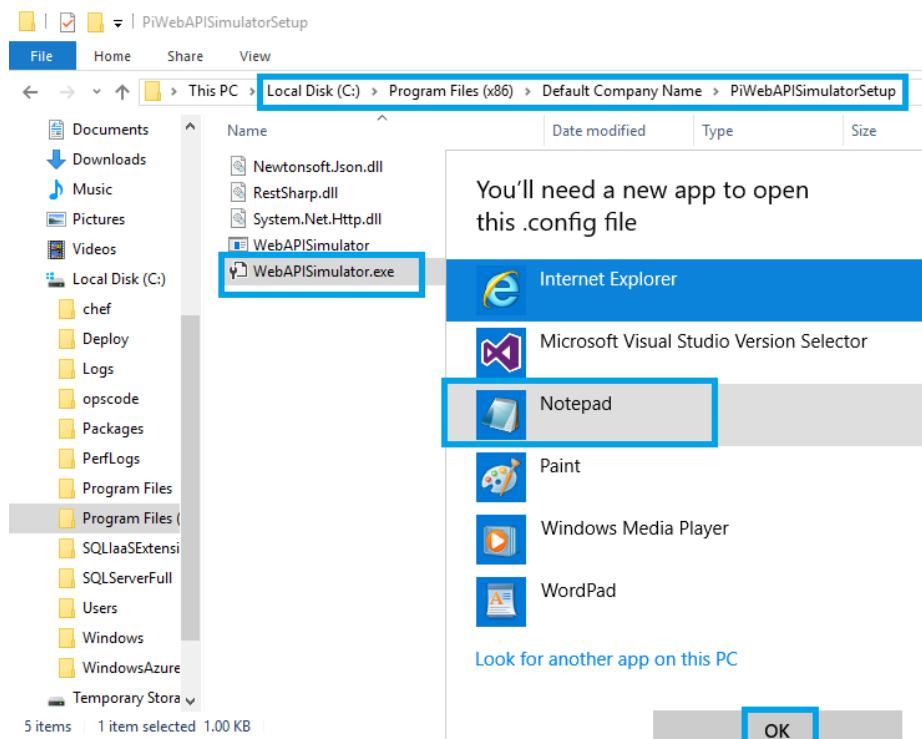
2. Navigate to the **Local Disk (C:) > Deploy > PIWebAPISimulatorSetup** and right-click to **Install**.



- 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"/>
```

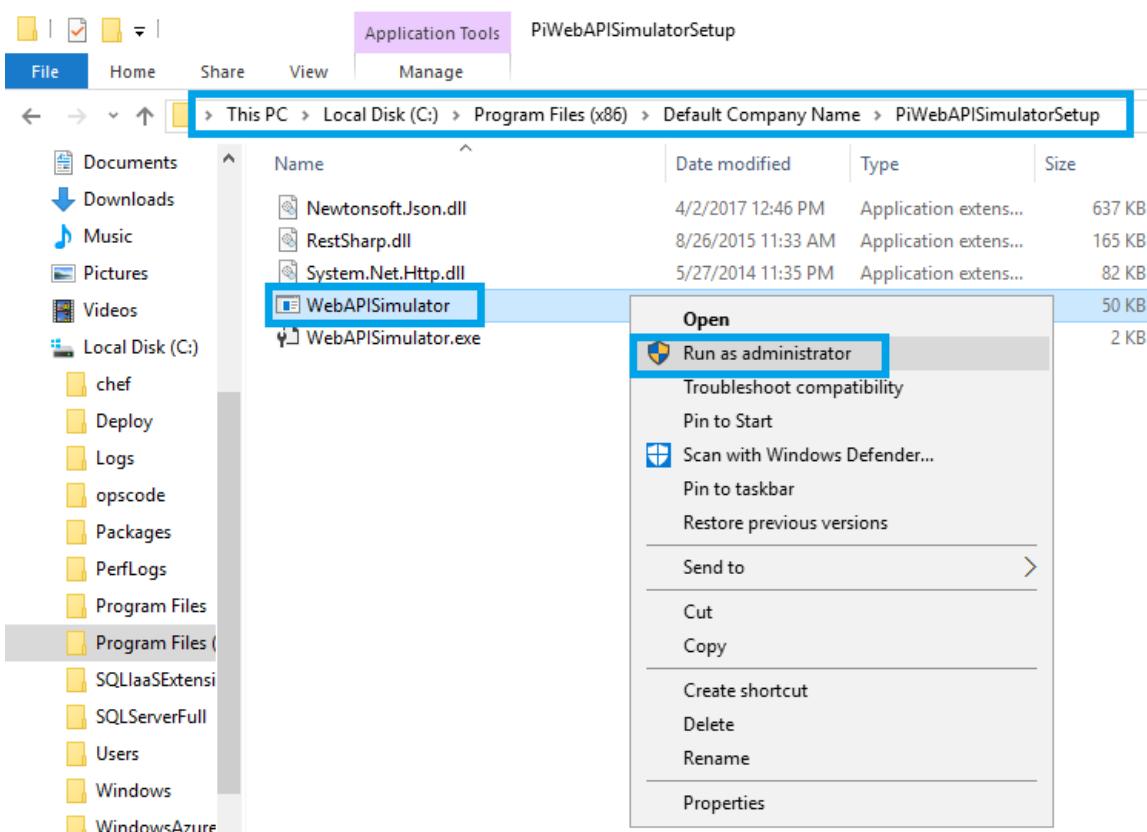
After updating all the values, click on **Save**.



The screenshot shows a Notepad window titled "WebAPISimulator.exe - Notepad". The content is an XML configuration file. A blue rectangular box highlights the following section of the code:

```
<appSettings>
  <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"/>
```

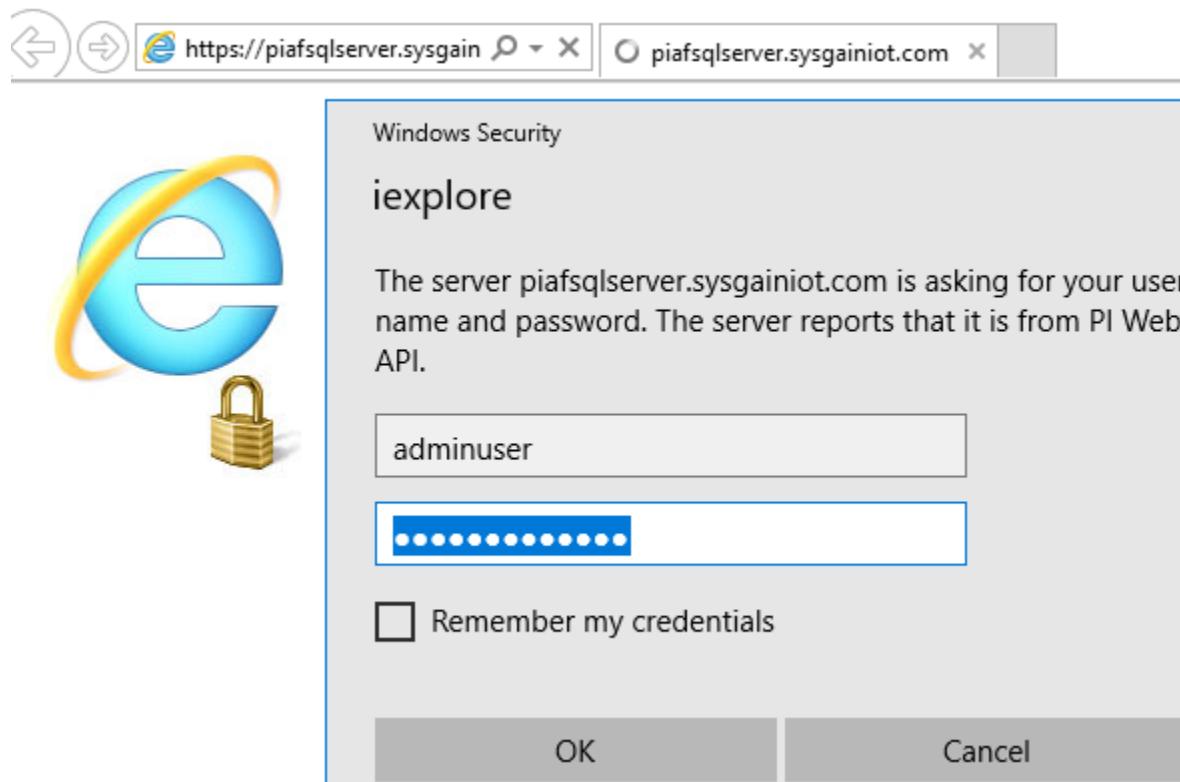
6. Navigate to **Local Disk (C:) > Program Files(X86) > Default Company Name > PiwebAPISimulatorSetup**. Select the **WebAPISimulator**, right click to **Run as Administrator**.



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

```
Select C:\Program Files (x86)\Default Company Name\PiWebAPISimulatorSetup\WebAPISimulator.exe
*****
Completed Status code is: Accepted
Status Description: Accepted
Done with processing of building :: Building 1
for powerscout P3716@2018
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** n-----n-----n-----
Completed Status code is: Accepted
Status Description: Accepted
for powerscout P3716@2020
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: Accepted
Status Description: Accepted
Done with processing of building :: Building 2
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: Accepted
Status Description: Accepted
Complete time entry: 9/24/2017 6:13:26 PM
=====Done with timestamp values, press any key to Exit
```

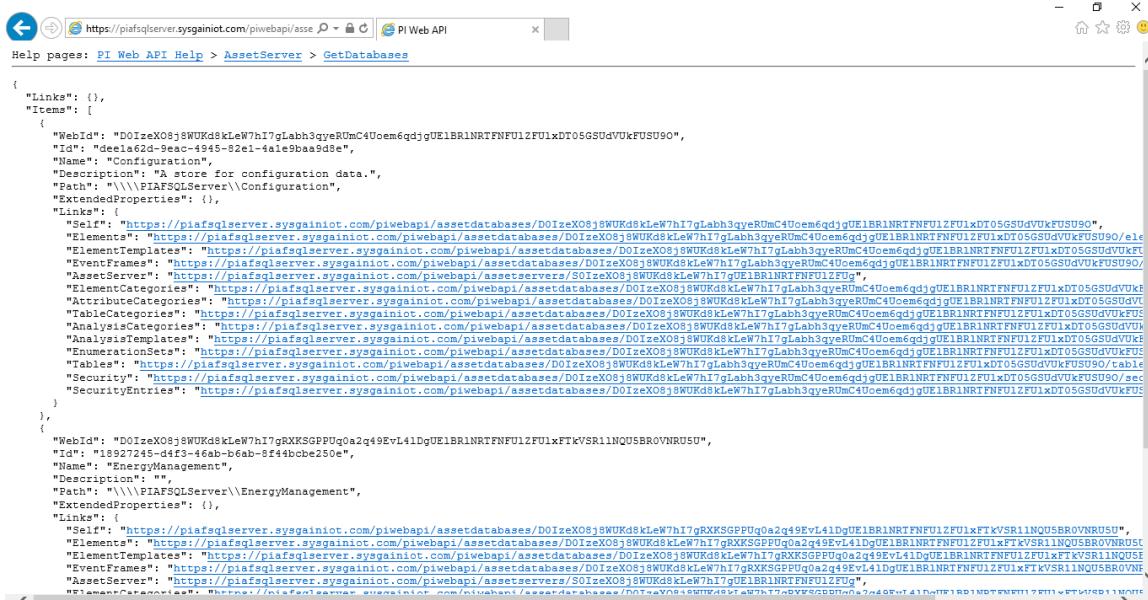
8. Paste the URL <https://piafsqlserver.sysgainiot.com/piwebapi/> in **Internet Explorer** to view the Data servers URLs. It will show a popup box like below. Enter PIAFSQLServer credentials to login.



Once you login you can view the asset servers urls 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



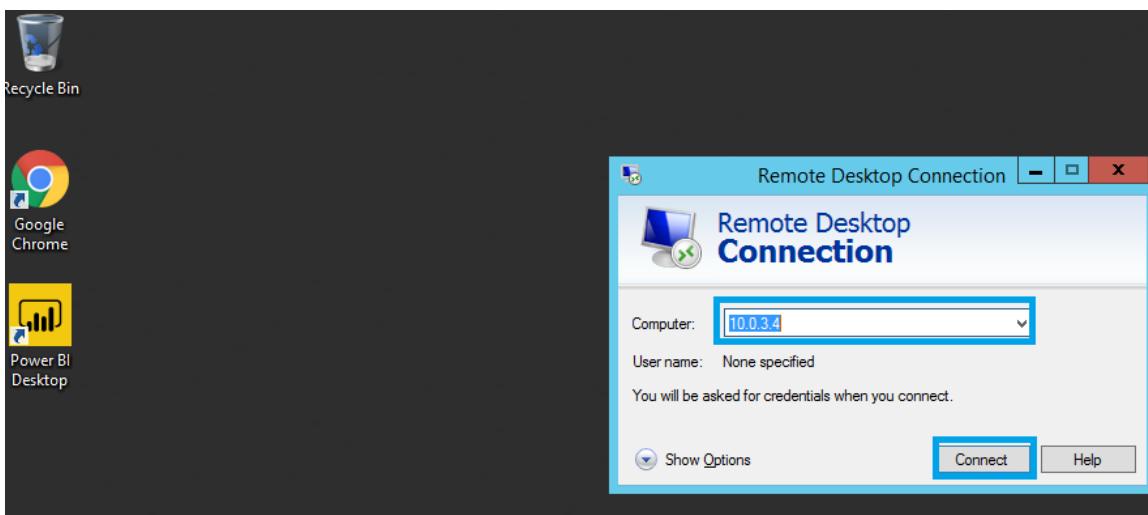
```

{
  "Links": {},
  "Items": [
    {
      "WebId": "DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
      "Id": "de1a62d-9eac-4945-82e1-4a1e9baa9d8e",
      "Name": "Configuration",
      "Description": "A store for configuration data.",
      "Path": "\\\PIAFSQLServer\\Configuration",
      "ExtendedProperties": {},
      "Links": [
        {
          "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90/elements",
          "ElementTemplates": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90/elementtemplates",
          "EventFrames": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90/eventframes",
          "AssetServer": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/SOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "AssetServerEntries": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/SOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "ElementCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "AttributeCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "TableCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "AnalysisCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "AnalysisTemplates": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "EnumerationSets": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90",
          "Tables": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90/table",
          "Security": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90/sec",
          "SecurityEntries": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTFNFU12FU1xDT05GSUdVUkFUSU90"
        }
      ],
      "WebId2": "DOIx08j8WUkd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTKvSR11NQ5BROVNRUSU",
      "Id2": "18927245-d4f3-46a8-b6ab-8f44bcbe250e",
      "Name2": "EnergyManagement",
      "Description2": "",
      "Path2": "\\\PIAFSQLServer\\EnergyManagement",
      "ExtendedProperties2": {},
      "Links2": [
        {
          "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIx08j8WUkd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTKvSR11NQ5BROVNRUSU"
        }
      ]
    }
  ]
}

```

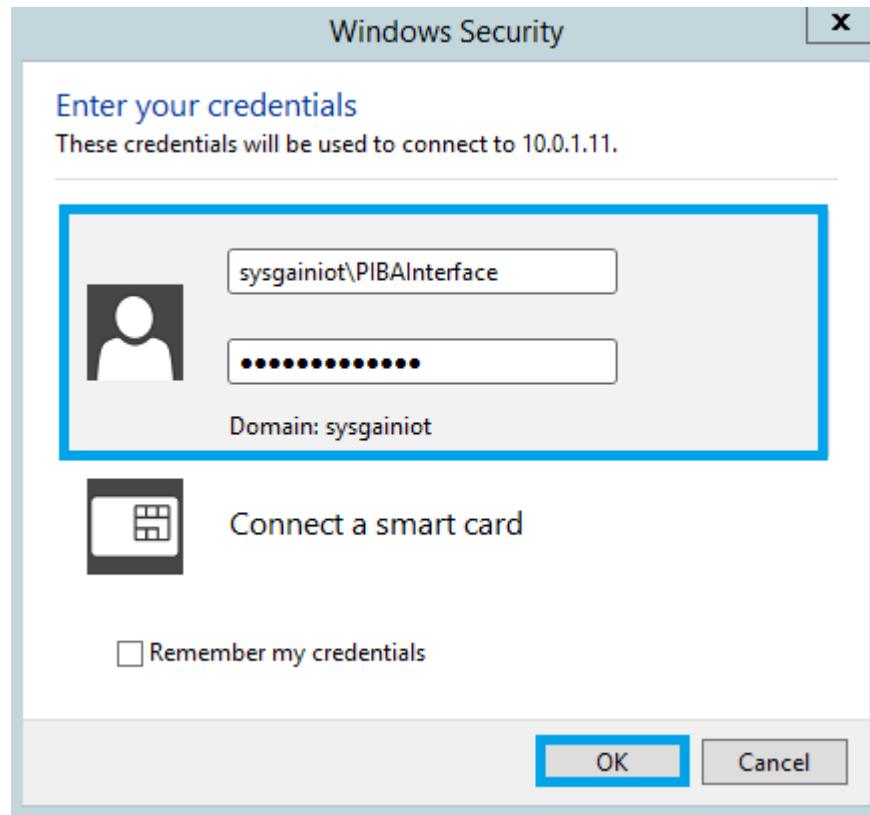
10. Installation of PI BA Integrator

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

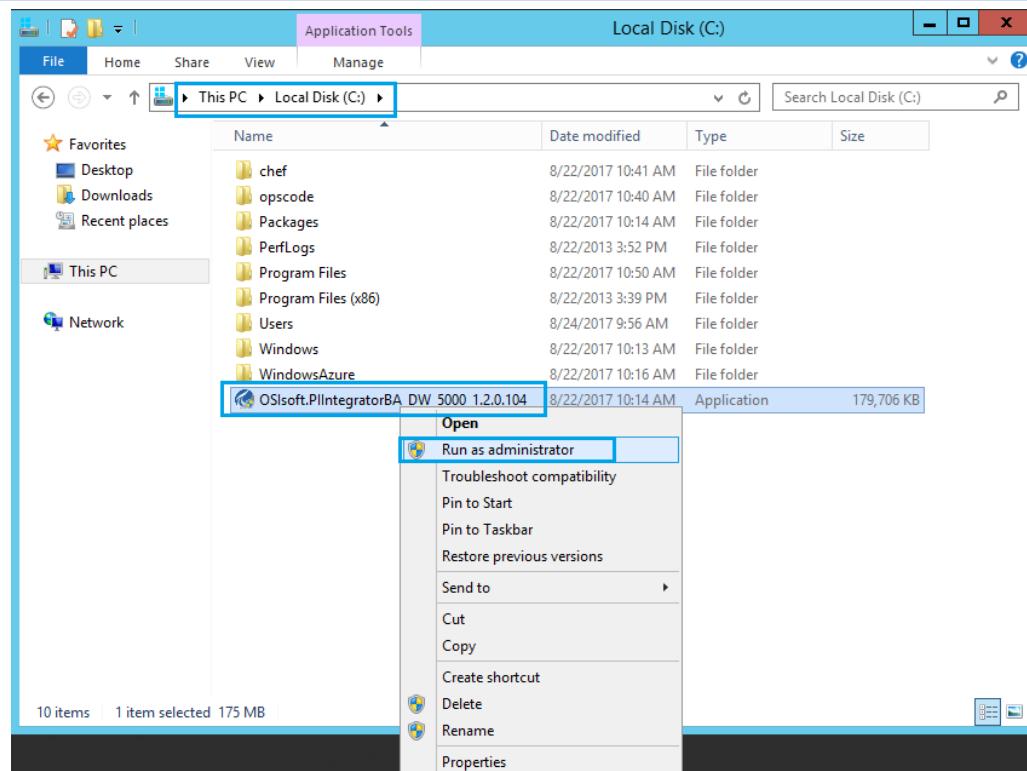


Note: Login with the **same** user credentials you created in the **ADServer**

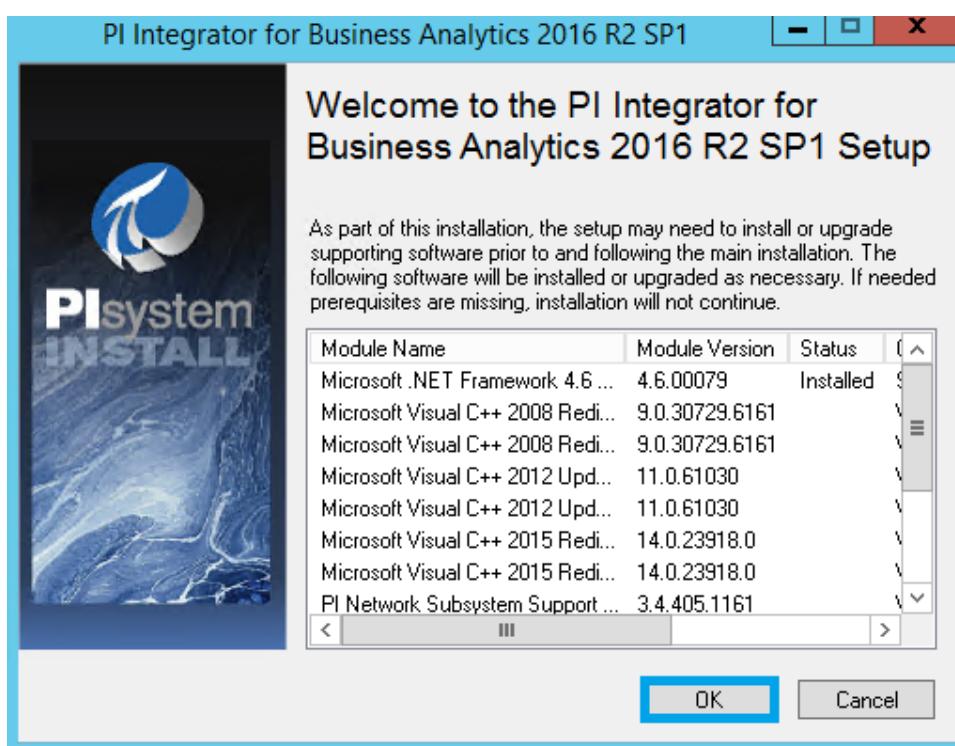
2. Login with credentials "**<domainname>\PIBAInterface**" (user you created in AD server) and **aq21password**.



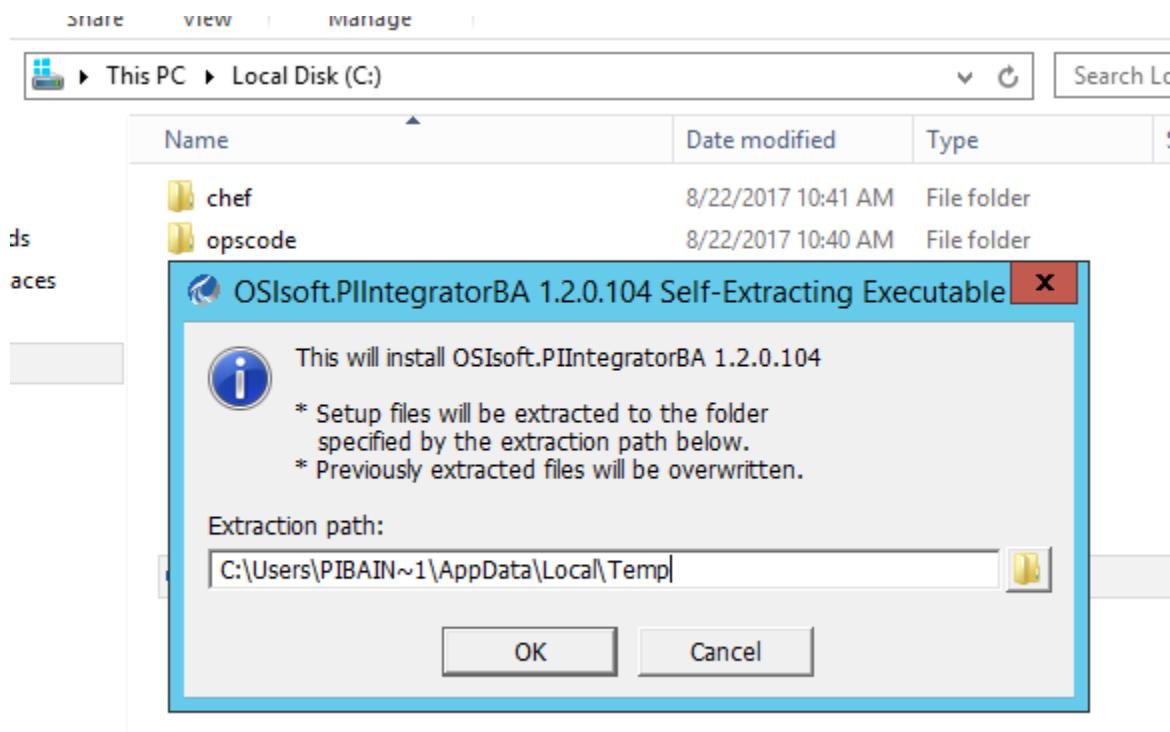
3. After connecting to the PIBA VMServer, navigate to the LocalDisk (C:) and select **OSISoft.PIIntegratorBA**, then right-click on and **Run as administrator**.



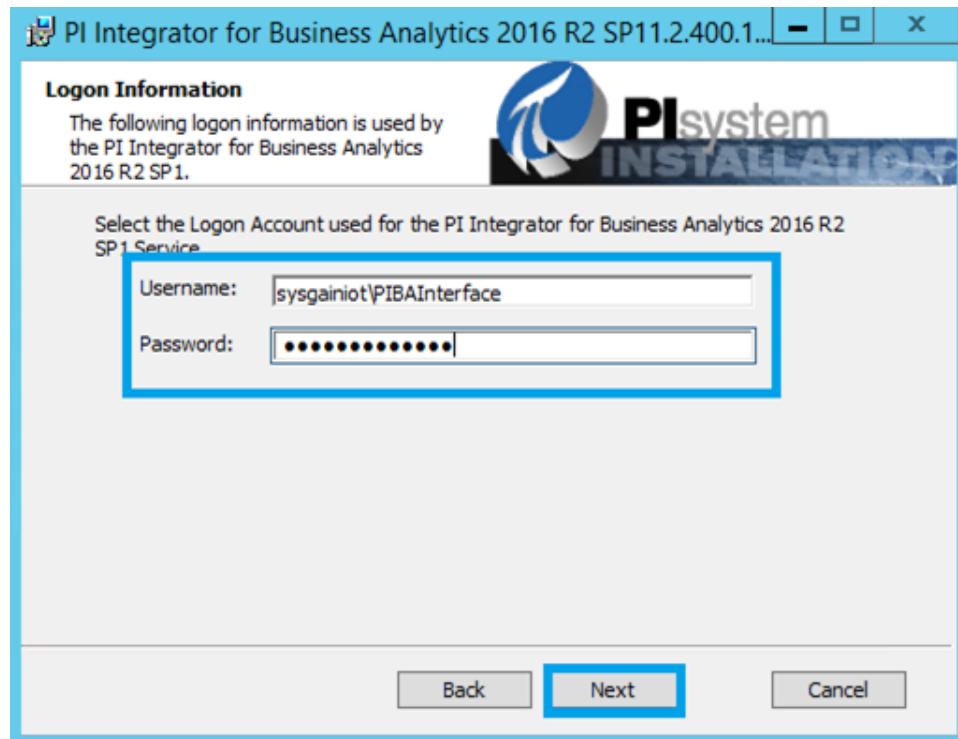
4. Click on **Ok**.



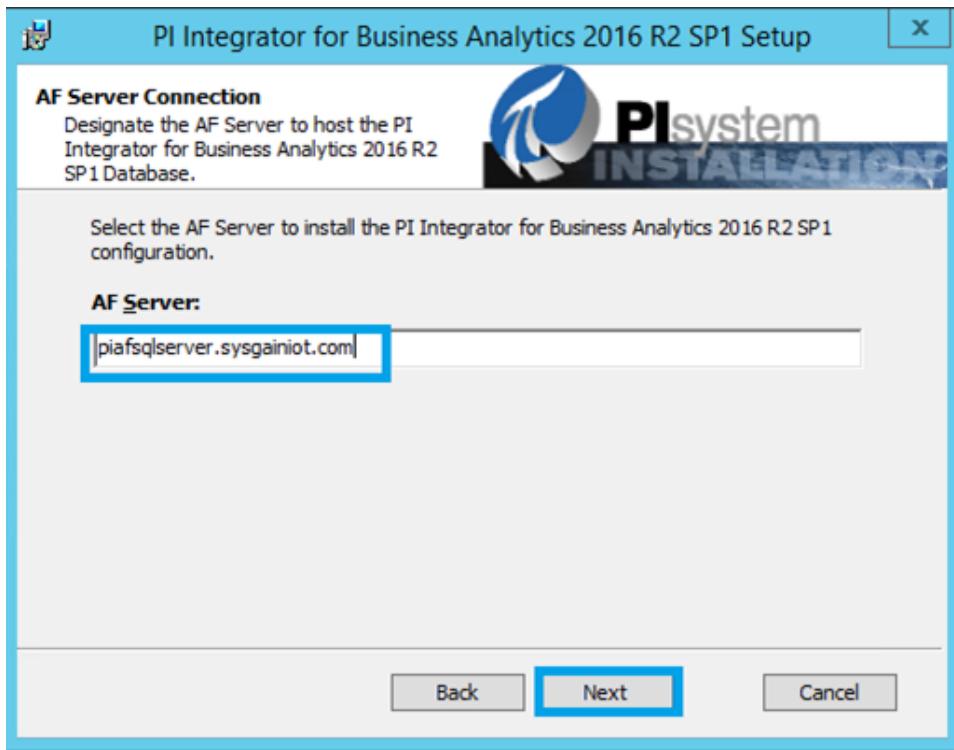
5. Click on **OK**



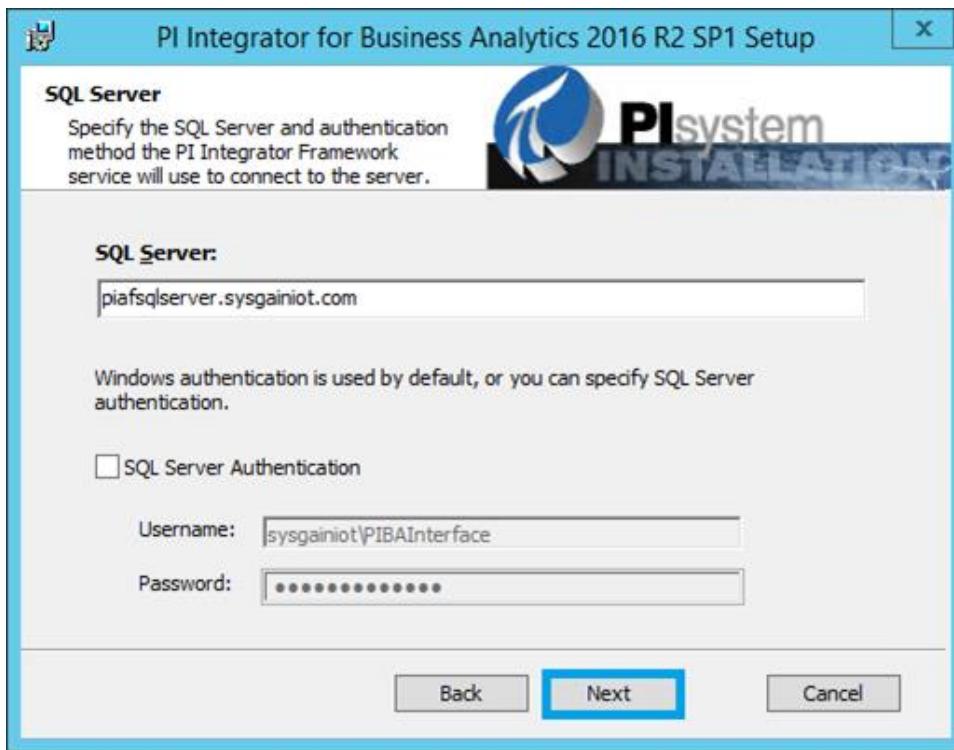
6. Give the same credentials which you used to login to PIBA server in Logon credentials and click on **Next**



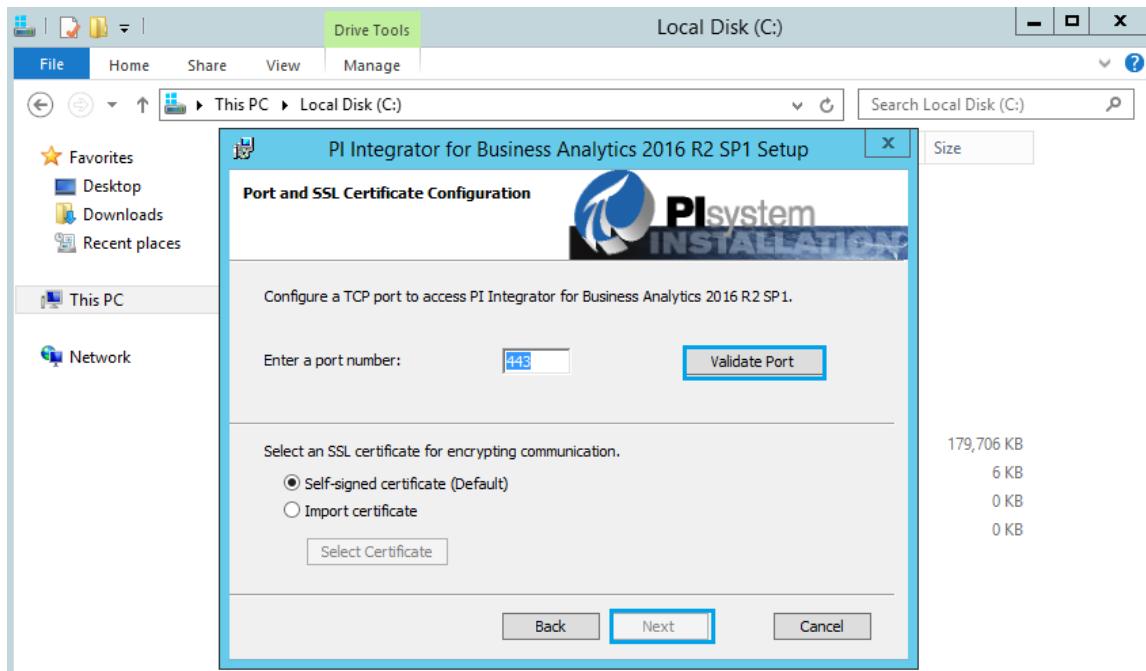
7. Give the AF sever link as piafsqlserver. <domainname> to host PIBA database and click on **Next**



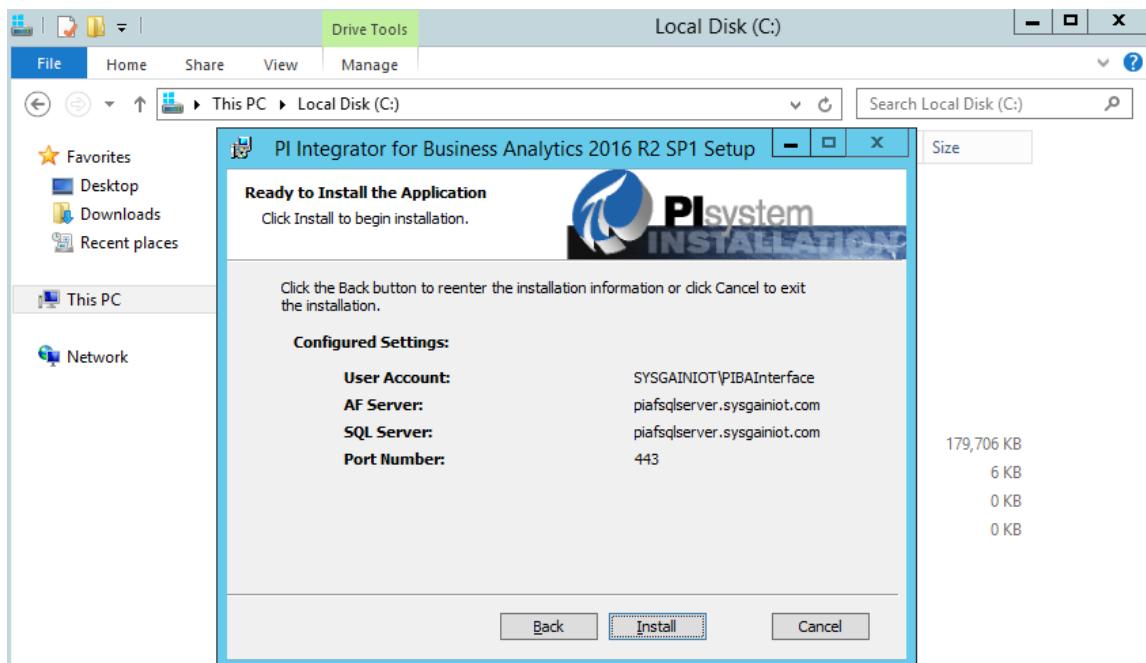
8. Click on **Next**



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

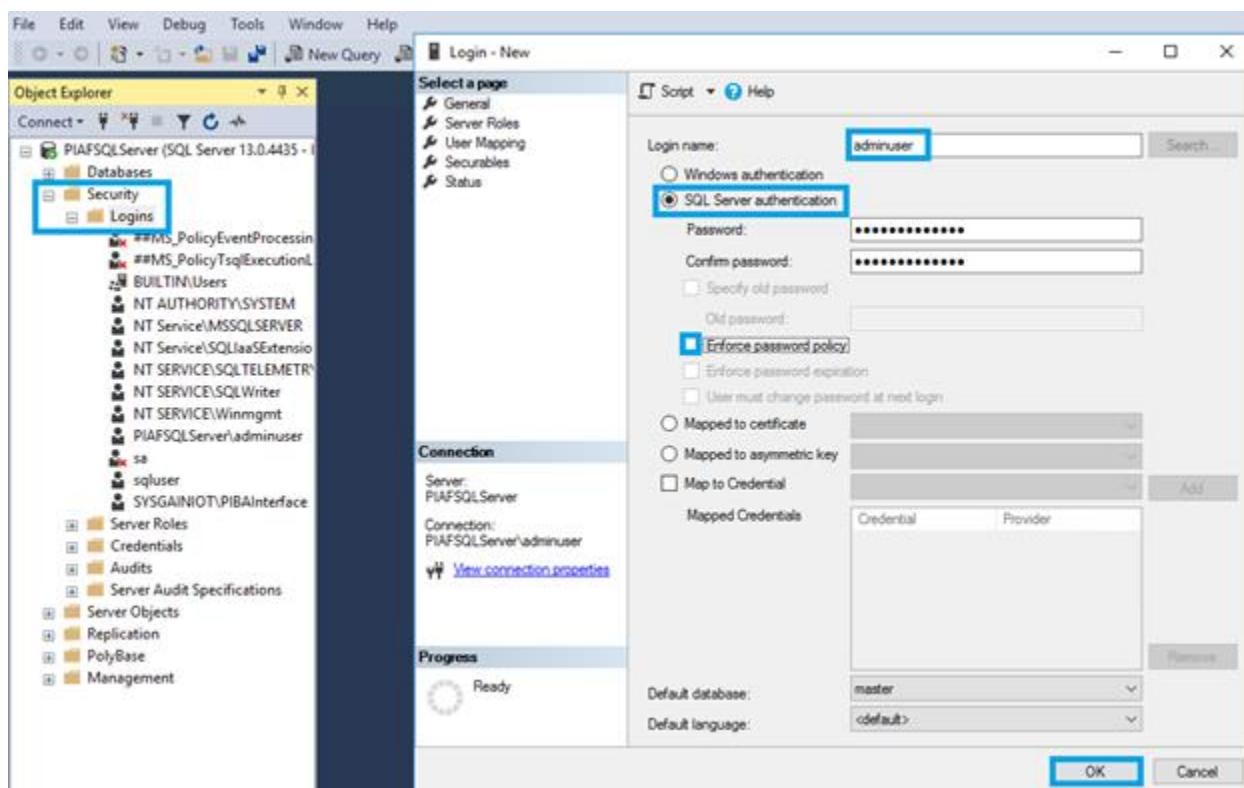


10. Click on **Install**.

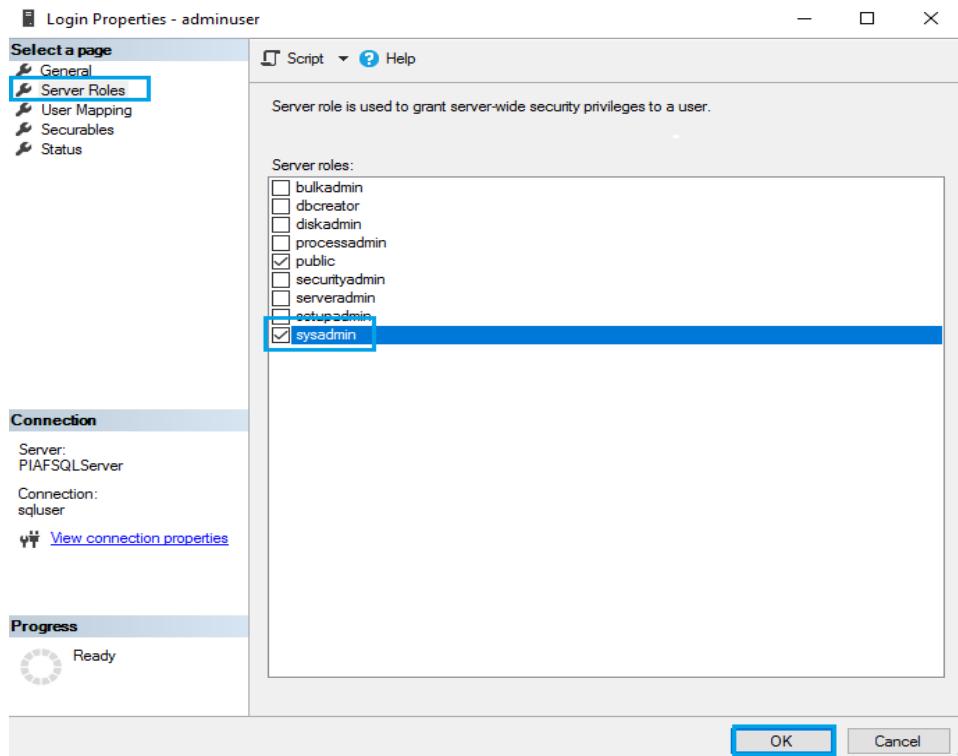


10.1. Configuring PI Business Analytics

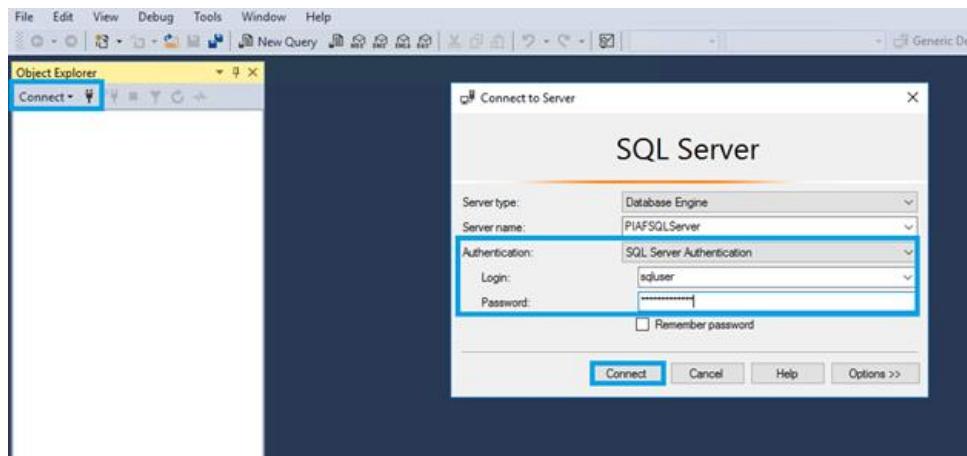
1. In Bastion Server, connect to the PIAFSQLServer with the credentials provided in the output section.
2. Go to the **Security** section, then right-click on **Login** and select **New Login**. Set the login name as **adminuser** and select **SQL Server Authentication**. Set a password and uncheck the box Enforce password policy, then click on **Ok**.



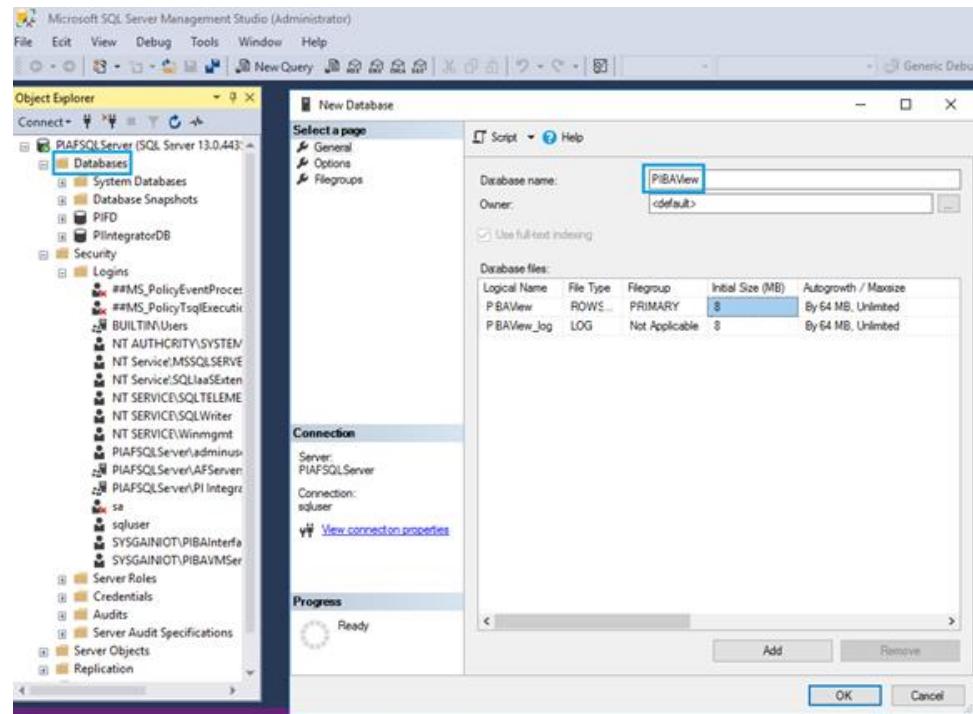
3. Right-click on the admin user under **Login** and select **Properties**. On the Properties screen, select **Server Roles**, then check **sysadmin** and click **Ok**.



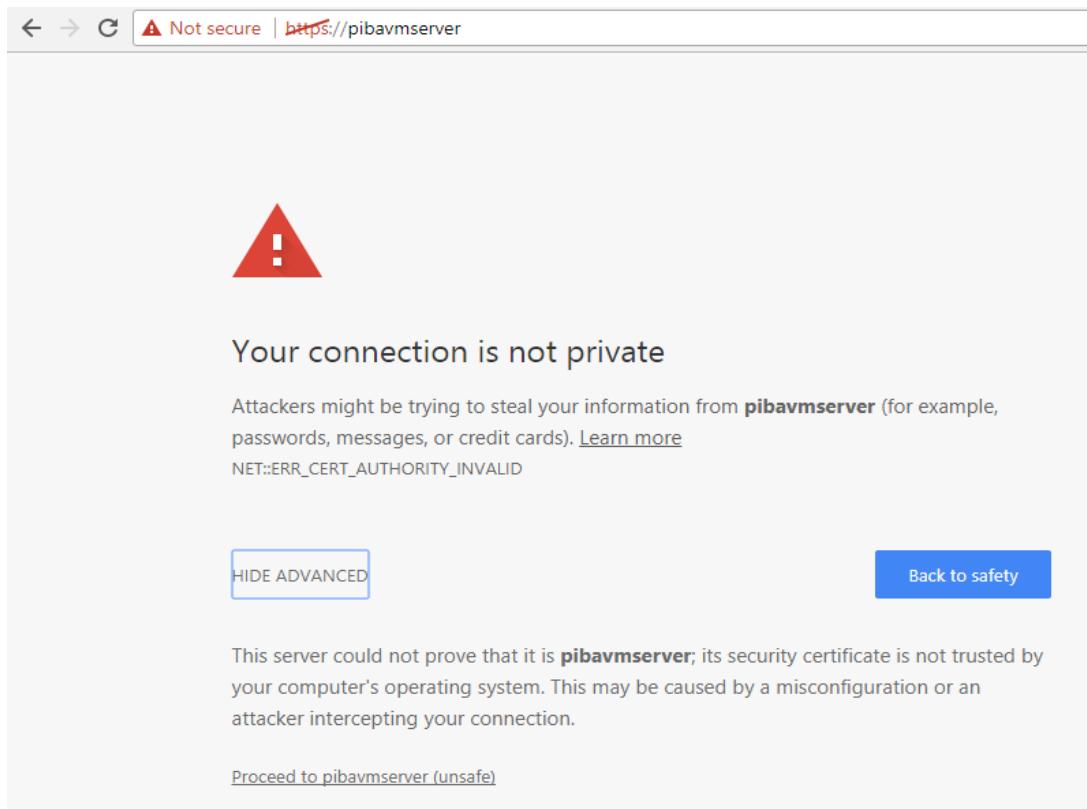
4. Disconnect and Click on connect in **ssms** to login with SQL Server authentication to create database with following SQL credentials



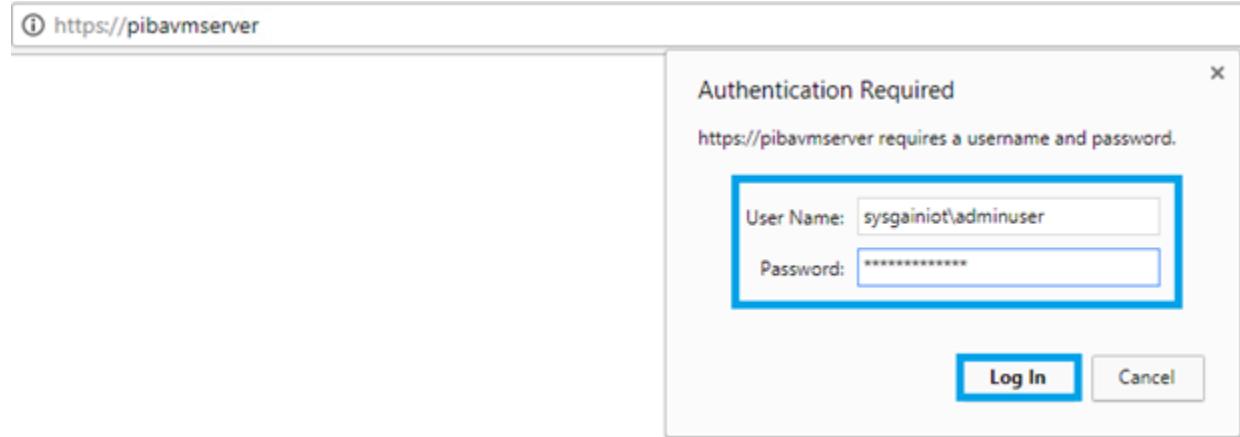
5. Go to the **SQLServer Management Studio**, right-click on **Database**, select **New Database**, and give the Database name as **PIBAView**. Click on **Ok**.



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.

← → ⌛ ⚠ Not secure | https://pibavmserver

☰

+ Create Asset View
Build a data view starting with your asset hierarchy + Create Event View
Build a data view starting with your event frame hierarchy MOD Modify View
Modify existing data view ✖ Remove View
Remove selected view

🔒	Name	Run Status	Type

3. Click on **Administration**.

← → ⌛ ⚠ Not secure | https://pibavmserver

☰ PI Integrator for Business Analytics
View
Build a data view starting with your hierarchy MOD Modify View
Modify existing data view ✖ Remove View
Remove selected view

📁 My Views
Manage your data views

>Create New Asset View
Build a data view starting with your asset hierarchy

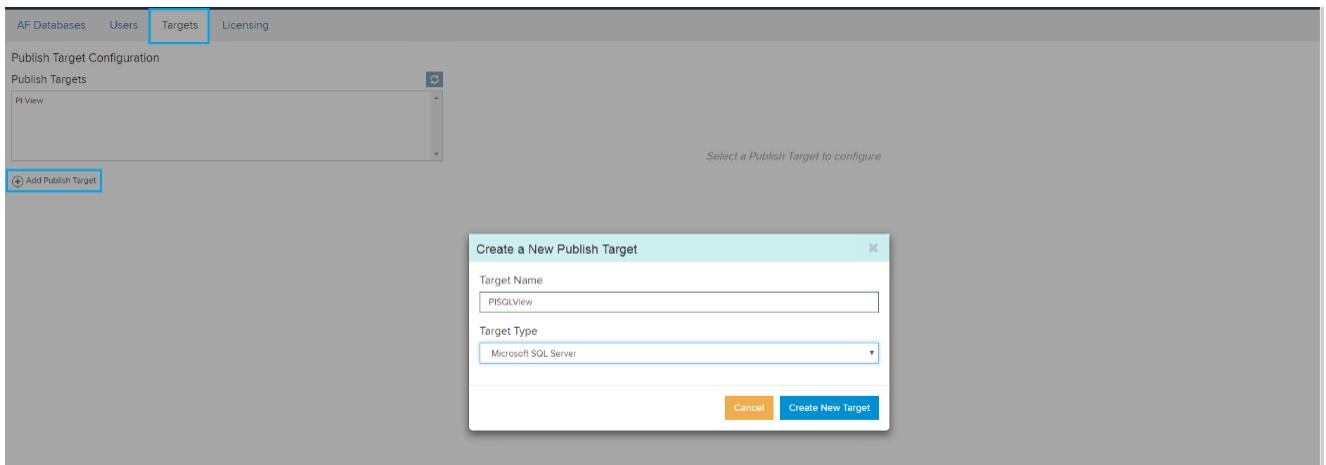
>Create New Event View
Build a data view starting with your event frame hierarchy

🔧 Administration
Manage servers users and targets

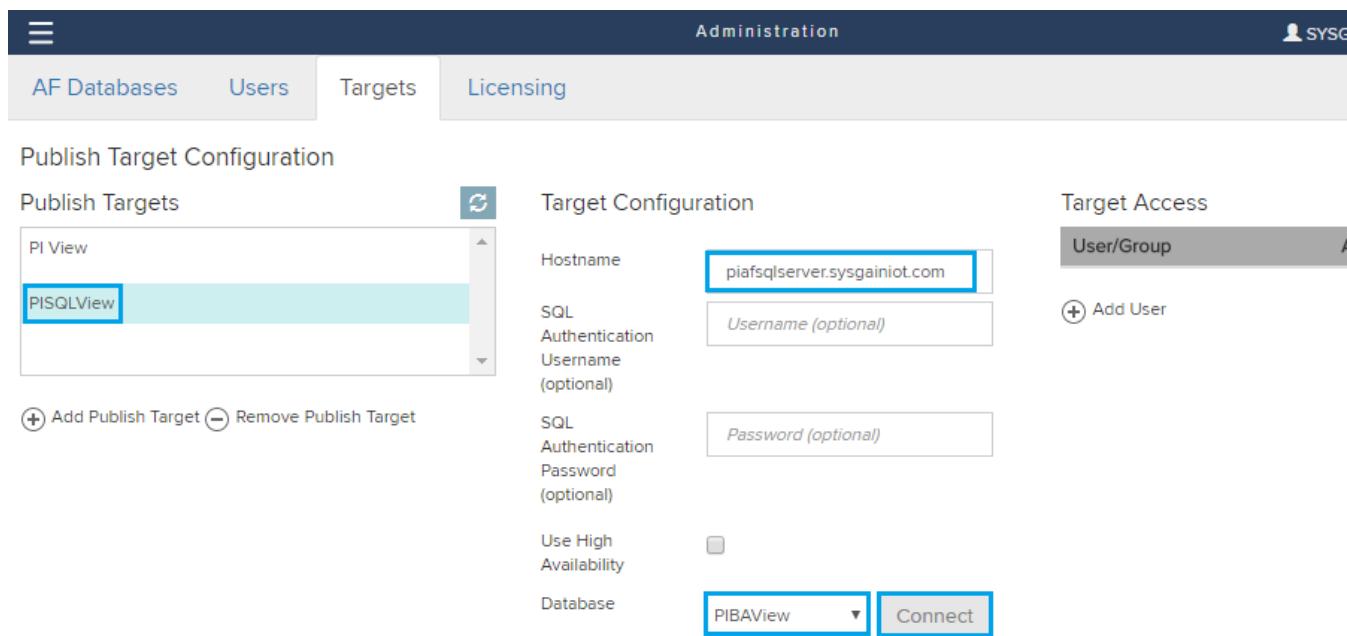
4. Select **Targets > Add Publish Target.**

Enter Target Name as **PISQLView**.

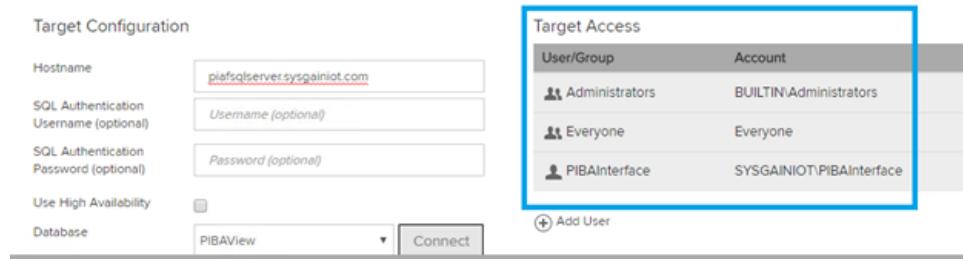
Select Target type as **Microsoft SQL Server** from drop down. After that click on create new target.



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**

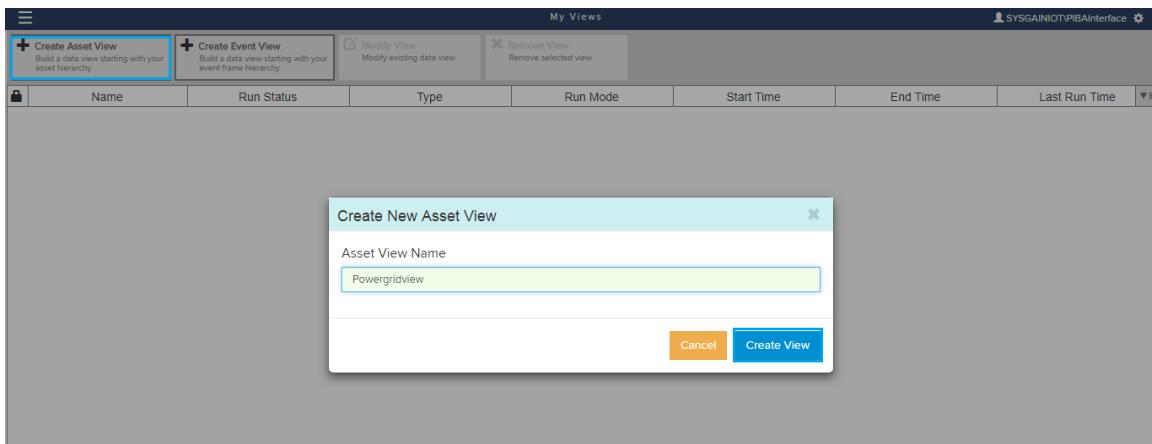


6. You can view the created **target access**



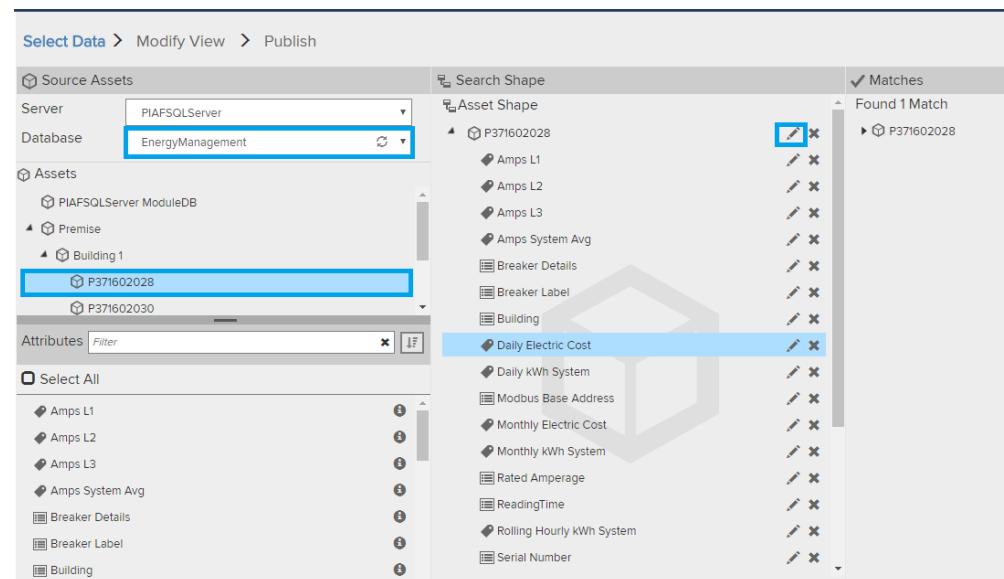
The screenshot shows two windows side-by-side. On the left is the 'Target Configuration' window, which includes fields for Hostname (piafsqlserver.sysgainiot.com), SQL Authentication Username (optional), SQL Authentication Password (optional), Use High Availability (checkbox), Database (PIBAView), and a 'Connect' button. On the right is the 'Target Access' window, which lists three entries: Administrators (Account: BUILTIN\Administrators), Everyone (Account: Everyone), and PIBAInterface (Account: SYSGAINIOT\PIBAInterface). A blue box highlights the 'Target Access' window.

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



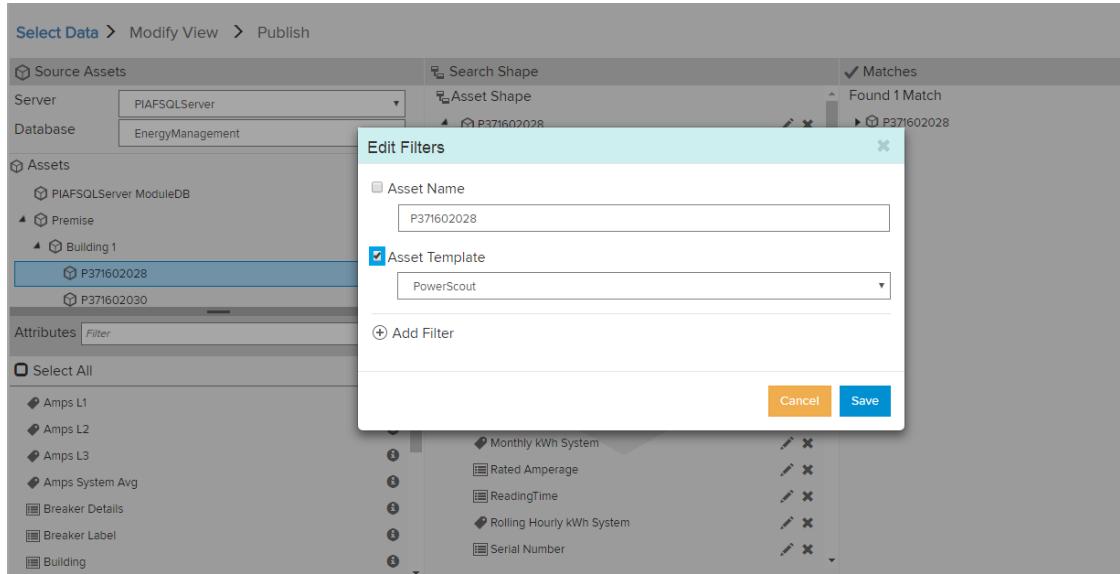
The screenshot shows a 'Create New Asset View' dialog box overlaid on a main interface. The dialog box has 'Asset View Name' set to 'Powergridview' and contains 'Cancel' and 'Create View' buttons. The main interface shows a toolbar with options like 'Create Asset View', 'Create Event View', 'Modify View', and 'Remove View'. Below the toolbar is a table with columns: Name, Run Status, Type, Run Mode, Start Time, End Time, and Last Run Time. The 'Create Asset View' button is highlighted with a blue box.

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**.

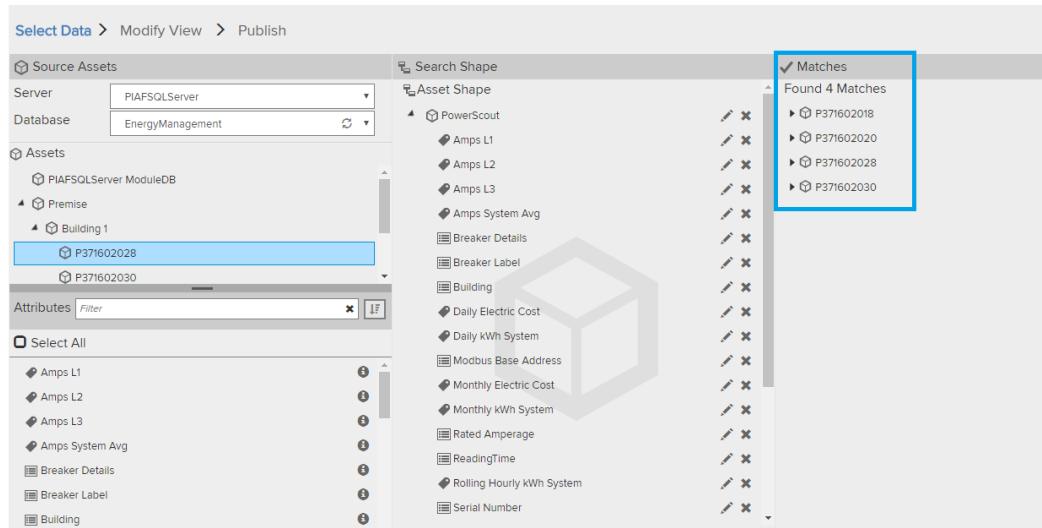


The screenshot shows the 'Select Data > Modify View > Publish' interface. In the 'Source Assets' section, 'Server' is set to 'PIAFSQLServer' and 'Database' is set to 'EnergyManagement'. Under 'Assets', 'Premise > Building 1 > P371602028' is selected. In the 'Attributes' section, several attributes are listed: Amps L1, Amps L2, Amps L3, Amps System Avg, Breaker Details, Breaker Label, Building, Daily Electric Cost, Daily kWh System, Modbus Base Address, Monthly Electric Cost, Monthly kWh System, Rated Amperage, ReadingTime, Rolling Hourly kWh System, and Serial Number. These attributes are being mapped to an 'Asset Shape' (P371602028) in the 'Search Shape' section. The 'Matches' section shows 'Found 1 Match' with 'P371602028' selected. A blue box highlights the 'Daily Electric Cost' attribute in the list.

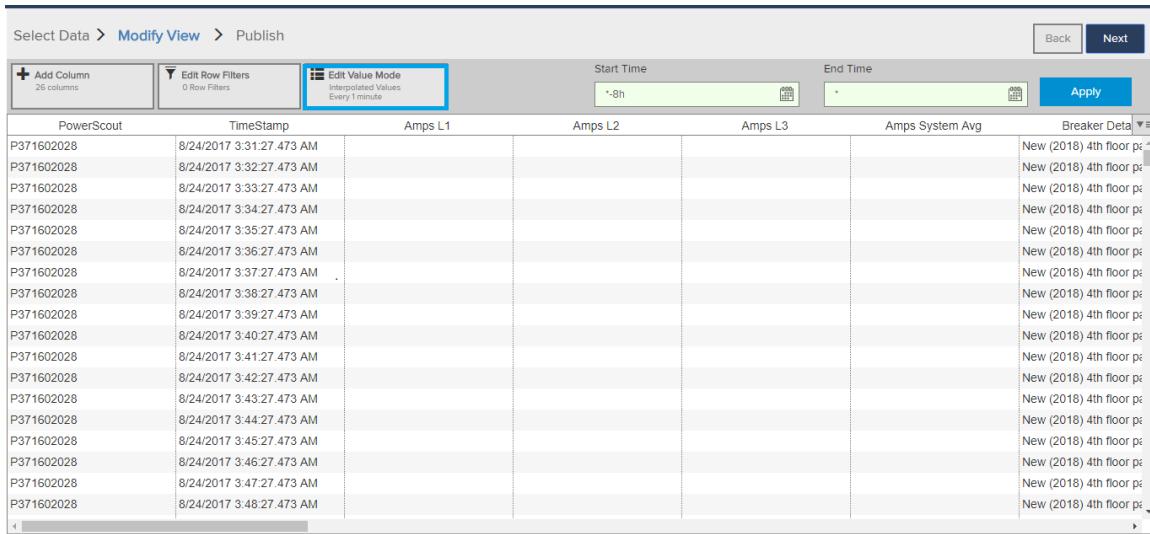
9. Click on edit near PI point **P371602028**, uncheck Asset name box, and check the **Assert Template** and **Save**.



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

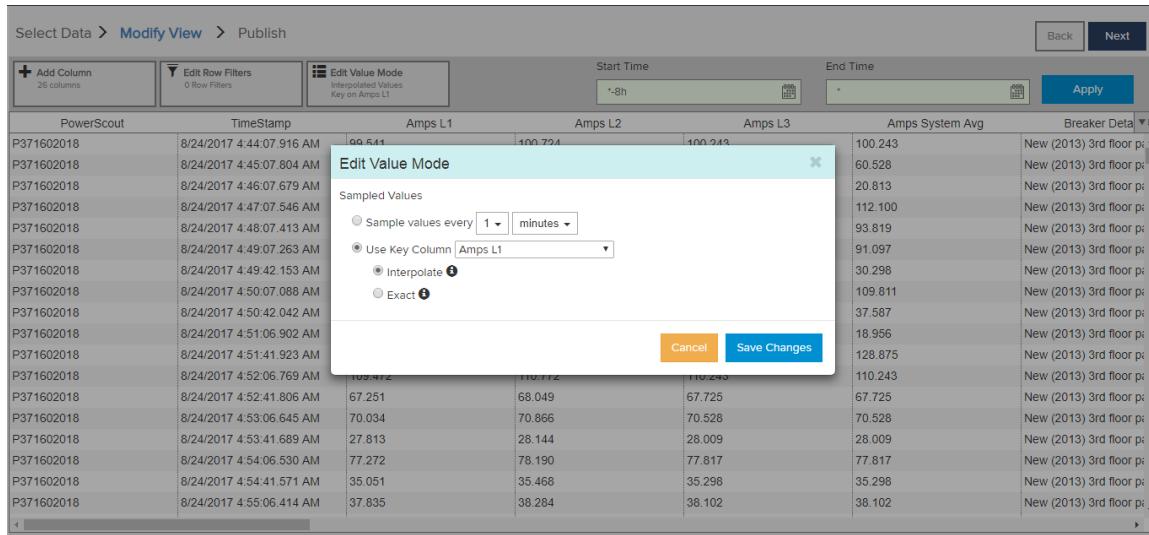


11. Click on **Edit Value Mode**.



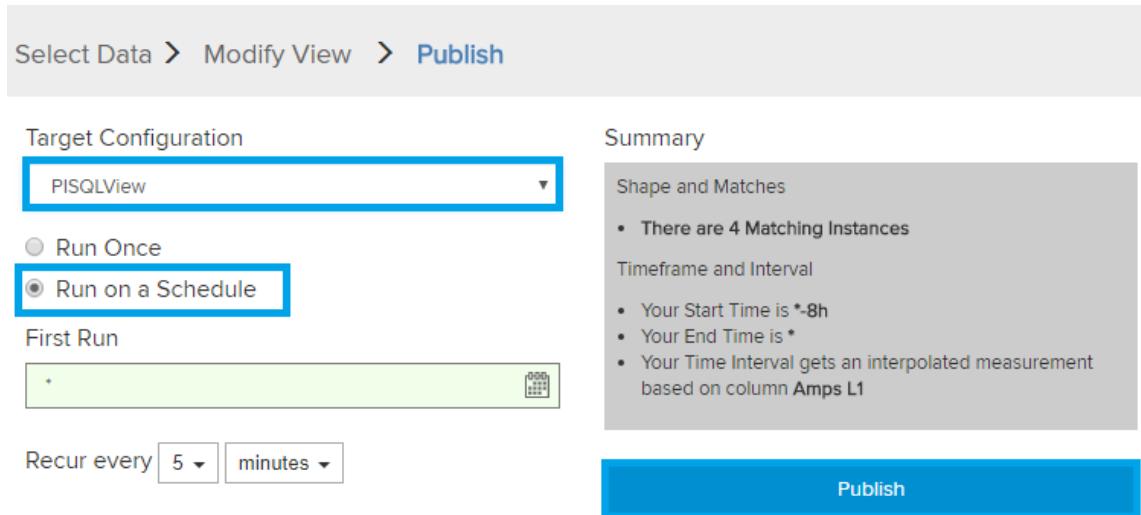
PowerScout	TimeStamp	Amps L1	Amps L2	Amps L3	Amps System Avg	Breaker Data
P371602028	8/24/2017 3:31:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:32:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:33:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:34:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:35:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:36:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:37:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:38:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:39:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:40:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:41:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:42:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:43:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:44:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:45:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:46:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:47:27.473 AM					New (2018) 4th floor p
P371602028	8/24/2017 3:48:27.473 AM					New (2018) 4th floor p

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



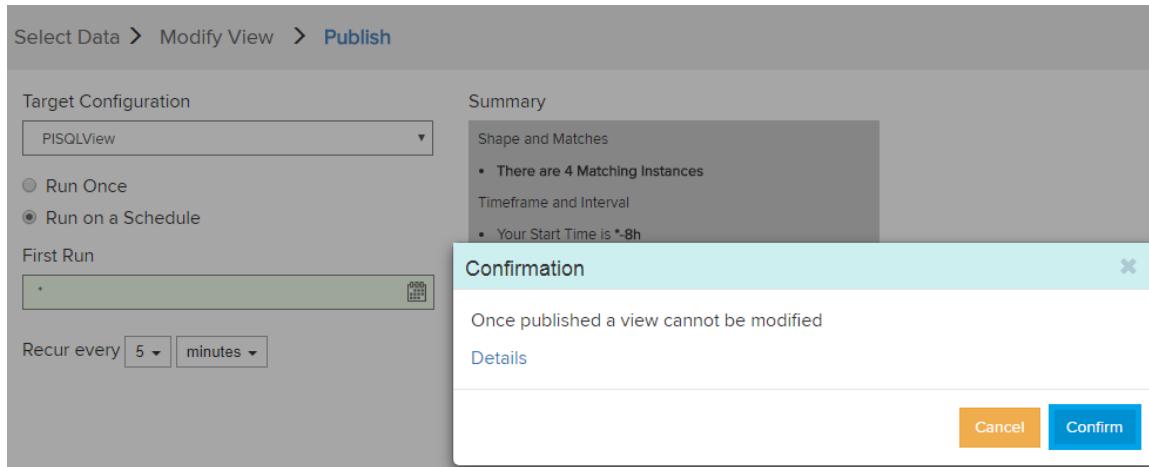
The screenshot shows a data grid with columns: PowerScout, TimeStamp, Amps L1, Amps L2, Amps L3, Amps System Avg, and Breaker Data. An 'Edit Value Mode' dialog box is open over the grid. The dialog has three options: 'Sample values every 1 minutes', 'Use Key Column Amps L1' (which is selected), and 'Interpolate'. There are 'Cancel' and 'Save Changes' buttons at the bottom.

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

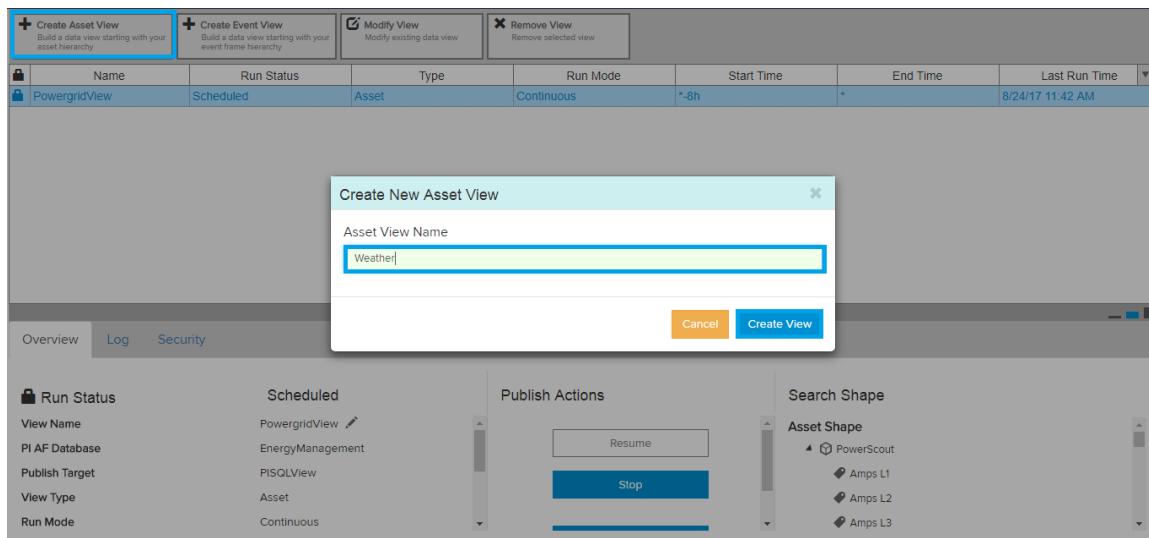


The screenshot shows the 'Publish' configuration screen. It includes sections for 'Target Configuration' (set to 'PISQLView'), 'Run Once' (radio button), 'Run on a Schedule' (radio button, selected), 'First Run' (empty field), 'Recur every 5 minutes' (dropdown), and a 'Summary' section. The 'Summary' section contains 'Shape and Matches' (4 Matching Instances) and 'Timeframe and Interval' (Your Start Time is *-8h, Your End Time is *). A large blue 'Publish' button is at the bottom right.

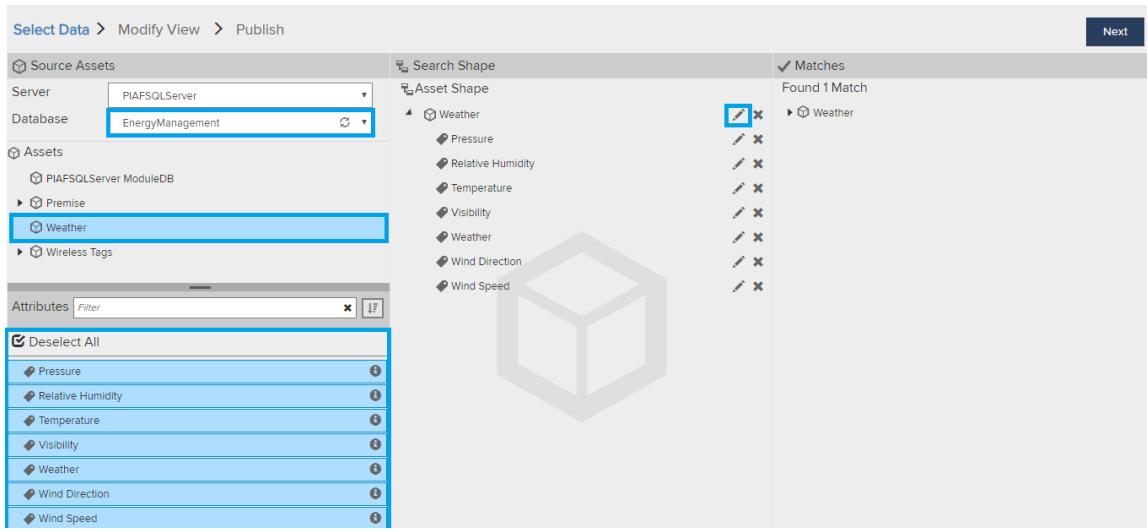
14. Click on **Confirm**.



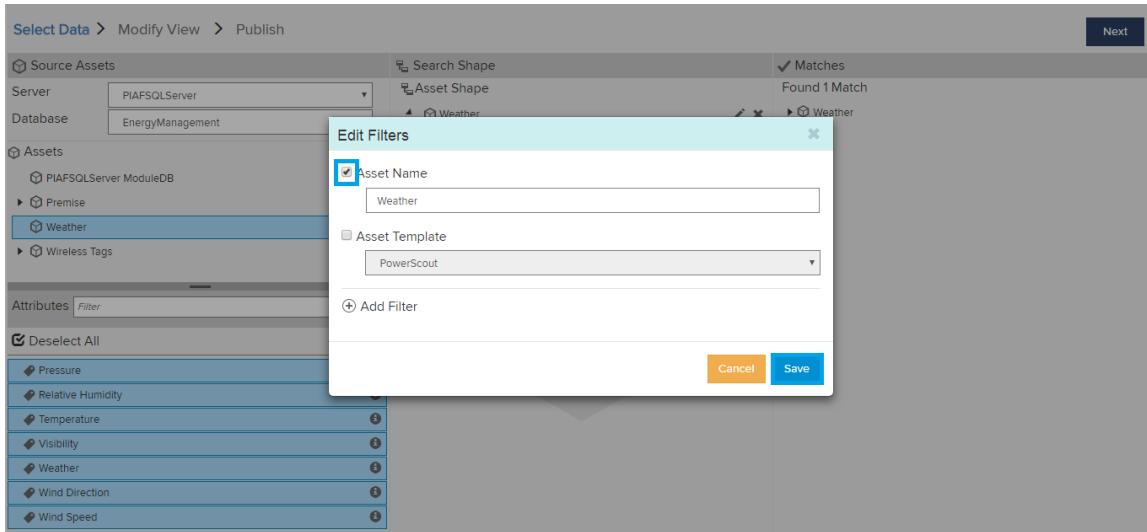
15. Create another Asset view by clicking on **Create asset view**, name it **Weather**, then click on **Create view**.



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.

Select Data > Modify View > Publish

Source Assets

- Server: PIAFSQLServer
- Database: EnergyManagement

Assets

- Premise
- Weather (selected)
- Wireless Tags

Attributes

- Pressure
- Relative Humidity
- Temperature
- Visibility
- Weather
- Wind Direction
- Wind Speed

Search Shape

- Asset Shape
- Weather
- Pressure
- Relative Humidity
- Temperature
- Visibility
- Wind Direction
- Wind Speed

Matches

- Weather
- Pressure
- Relative Humidity
- Temperature
- Visibility
- Wind Direction
- Wind Speed

Next

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

Select Data > Modify View > Publish

Edit Value Mode

Interpolated Values
Key on Pressure

	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Wind Direction	Wind Speed
Weather	8/24/2017 4:48:07 4...	29.207	30.174	54.801	3.047	Overscast	North	7.241
Weather	8/24/2017 4:49:07 3...	31.213					Variable	19.281
Weather	8/24/2017 4:49:42 2...	31.922					Light ...	23.531
Weather	8/24/2017 4:50:07 1...	29.220					Northwest	
Weather	8/24/2017 4:50:42 1...	30.709					North	7.320
Weather	8/24/2017 4:51:06 9...	29.011					Fog/Mist	16.255
Weather	8/24/2017 4:51:41 9...	30.932					Southeast	
Weather	8/24/2017 4:52:06 8...	28.928					North	6.064
Weather	8/24/2017 4:52:41 8...	29.719					Southeast	17.590
Weather	8/24/2017 4:53:06 7...	31.715					West	5.566
Weather	8/24/2017 4:53:41 7...	28.506					Breezy	10.314
Weather	8/24/2017 4:54:06 5...	31.938					South	
Weather	8/24/2017 4:54:41 6...	30.639	65.982	72.929	6.598		Wind in Vic...	22.290
Weather	8/24/2017 4:55:06 4...	28.160	4.002	36.361	0.400		West	3.038
Weather	8/24/2017 4:55:41 5...	30.862	71.546	76.212	7.155		Northwest	23.625
Weather	8/24/2017 4:56:06 3...	30.947	73.686	77.474	7.369		Light Rain Fog/Mist	15.836
Weather	8/24/2017 4:56:41 3...	28.214	5.349	37.156	0.535		Light Rain	0.960
Weather	8/24/2017 4:57:06 2...	29.735	43.369	59.588	4.337		A Few Clouds	17.171
Weather	8/24/2017 4:57:41 2...	28.437	10.913	40.439	1.091		South	17.685
							unknown Precip	1.284
							Fair and Breezy	10.409
							A Few Clouds	2.619

Edit Value Mode

Sampled Values

Sample values every 1 minutes

Use Key Column Pressure

Interpolate

Exact

Cancel Save Changes

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

Select Data > Modify View > Publish

Start Time: *-1h End Time: *

Apply

Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	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 Vic...	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**.

Select Data > Modify View > Publish

Target Configuration: PISQLView

Summary

Shape and Matches

- There are 1 Matching Instances

Timeframe and Interval

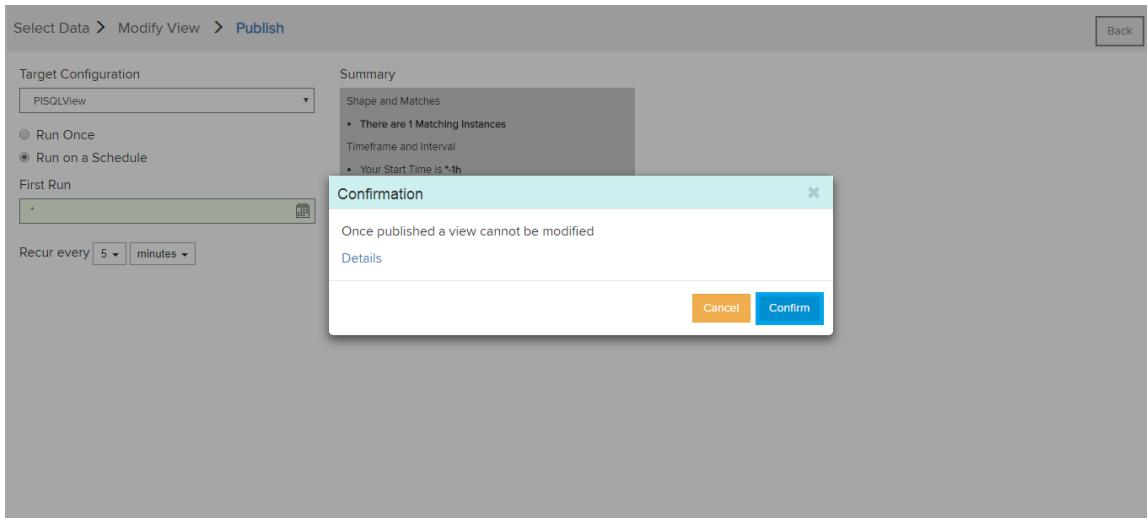
- Your Start Time is *-1h
- Your End Time is *
- Your Time Interval gets an interpolated measurement based on column Pressure

First Run

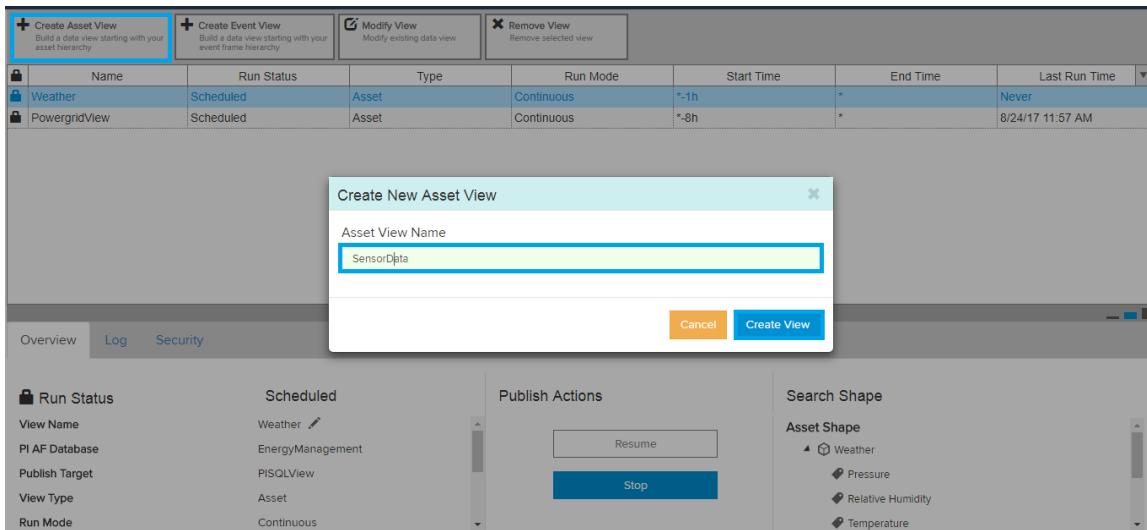
Recur every 5 minutes

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**.

Select Data > Modify View > Publish

Source Assets

Server: PIAFSQLServer
Database: EnergyManagement

Assets

- PIAFSQLServer ModuleDB
- Premise
- Weather
- Wireless Tags
 - Light Sensor 1

Attributes

Filter: Brightness, Humidity, Name, Temperature

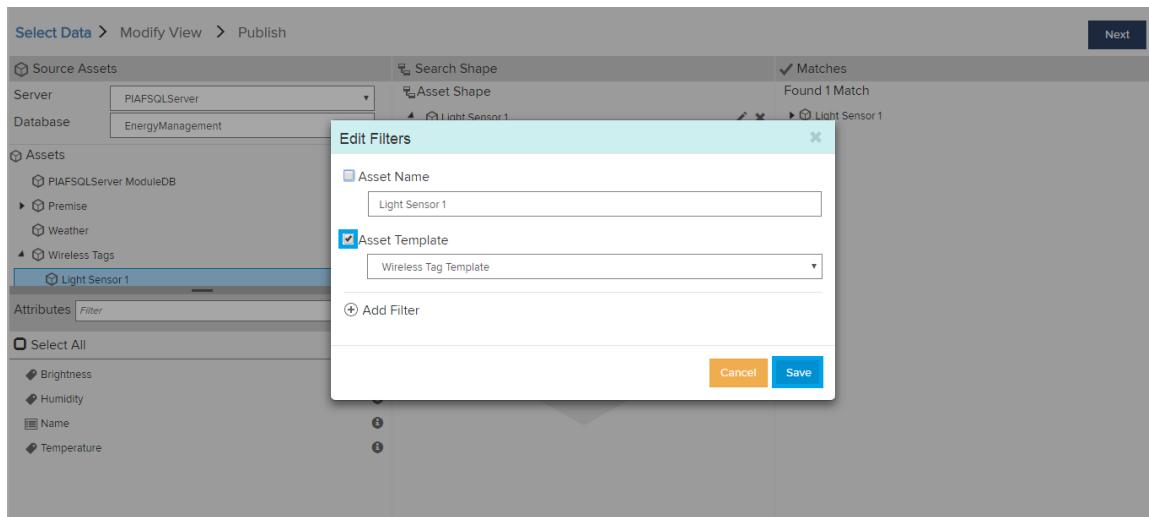
Edit Filters

Asset Name: Light Sensor 1
Asset Template: Wireless Tag Template

Matches

Found 1 Match: Light Sensor 1

Next



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

Select Data > Modify View > Publish

Source Assets

Server: PIAFSQLServer
Database: EnergyManagement

Assets

- PIAFSQLServer ModuleDB
- Premise
- Weather
- Wireless Tags
 - Light Sensor 1

Attributes

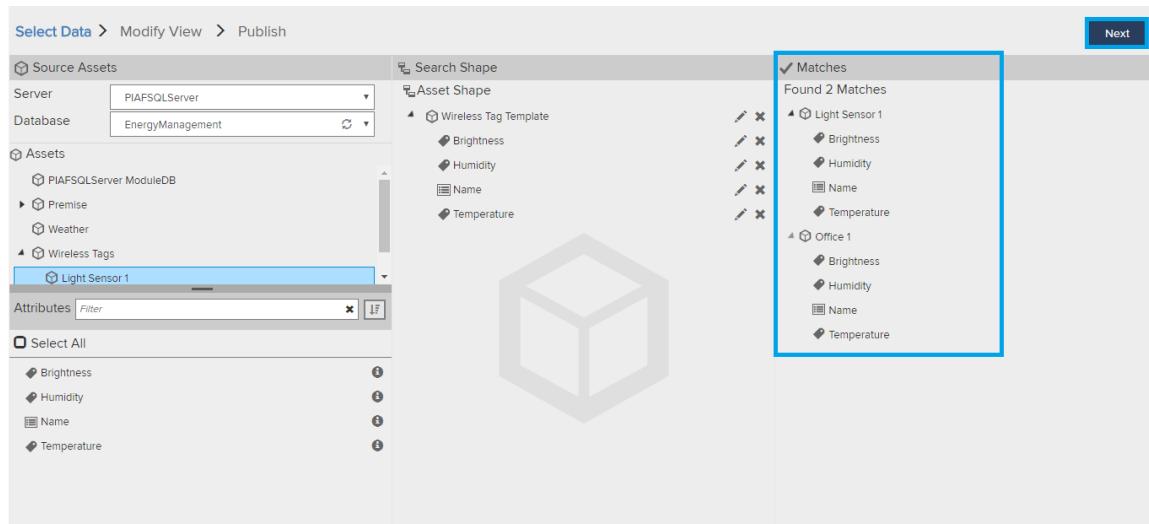
Filter: Brightness, Humidity, Name, Temperature

Matches

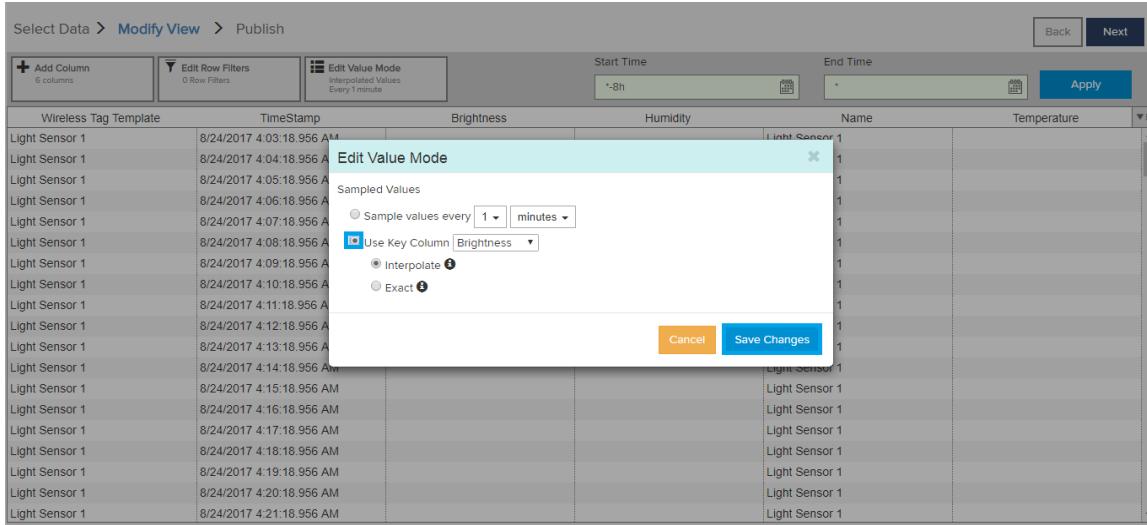
Found 2 Matches

- Light Sensor 1
 - Brightness
 - Humidity
 - Name
 - Temperature
- Office 1
 - Brightness
 - Humidity
 - Name
 - Temperature

Next

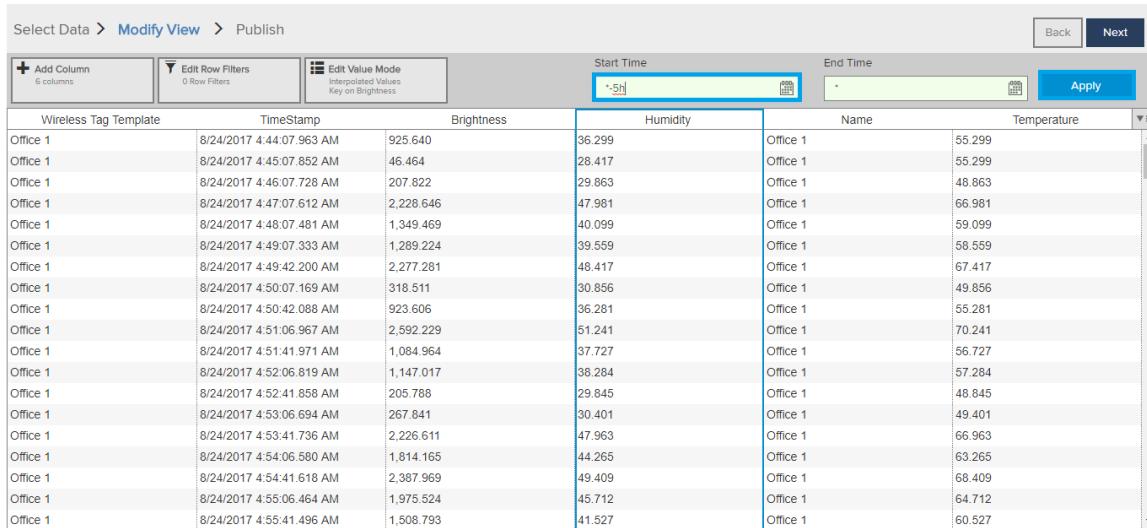


26. Click on **Edit Value Mode**, select **Use Key Column**, and **Save Changes**.



Wireless Tag Template	TimeStamp	Brightness	Humidity	Name	Temperature
Light Sensor 1	8/24/2017 4:03:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:04:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:05:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:06:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:07:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:08:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:09:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:10:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:11:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:12:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:13:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:14:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:15:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:16:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:17:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:18:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:19:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:20:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:21:18.956 AM			Light Sensor 1	

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	926.640	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**.

Select Data > Modify View > Publish

Target Configuration

PISQLView

Run Once

Run on a Schedule

First Run

*

Summary

Shape and Matches

- There are 2 Matching Instances

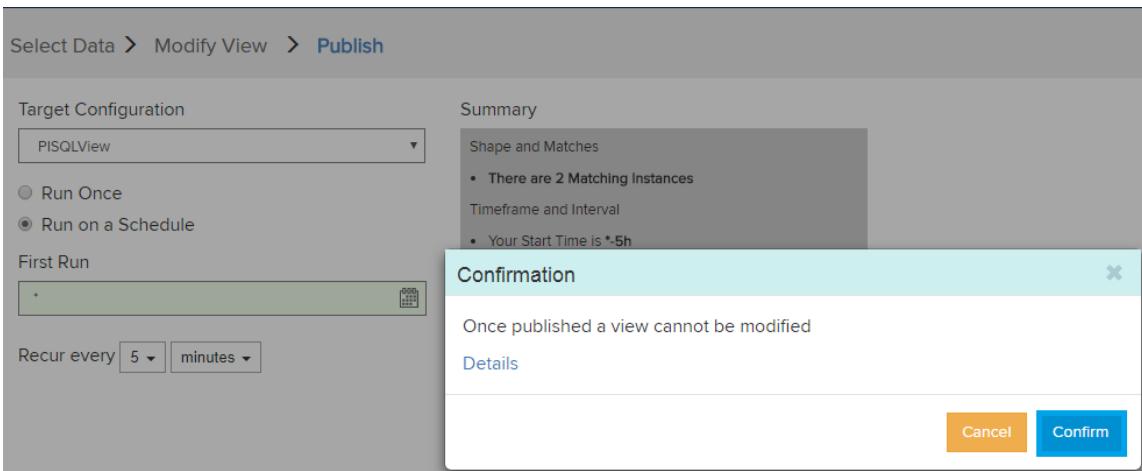
Timeframe and Interval

- Your Start Time is *-5h
- Your End Time is *
- Your Time Interval gets an interpolated measurement based on column Brightness

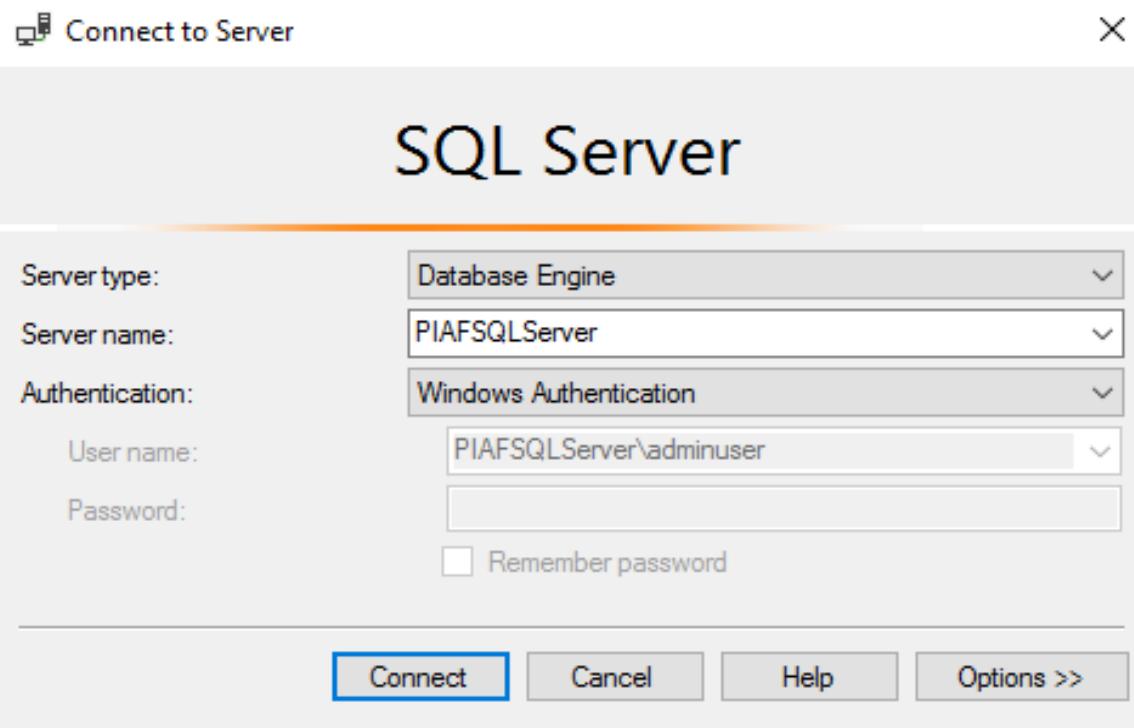
Recur every minutes

Publish

29. Click on **Confirm**.



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

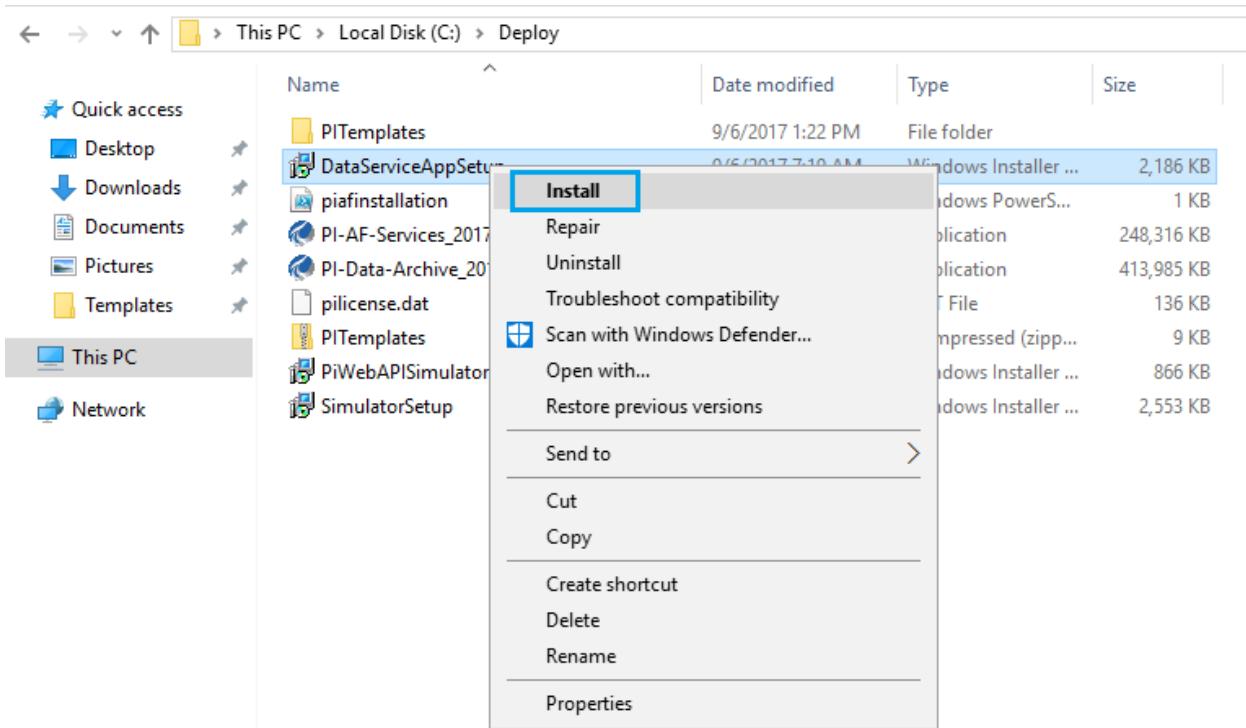


31. you must navigate to the **PIBAView** database > **Tables** and right click on any of the tables, then click on **Select Top 1000 Rows**.

ID	Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather
1	Weather	2017-08-24 04:44:07.980	30.7119654764943	67.7991369123567	74.001490782904	6.77991369123567	Light Rain Fog/Mat	
2	Weather	2017-08-24 04:45:07.870	28.844827232759	21.120680318946	46.461201680178	2.1120680318946	Mostly Cloudy	
3	Weather	2017-08-24 04:46:07.747	31.6321701387093	90.8042534677331	87.5745095459626	9.08042534677332	Thunderstorm Light Rain	
4	Weather	2017-08-24 04:47:07.627	30.4195130441429	60.4878261035717	69.687826174011073	6.04878261035717	Fair and Windy	
5	Weather	2017-08-24 04:48:07.497	29.206855945764	30.1713987394103	51.801252562521	3.01713987394103	Overcast	
6	Weather	2017-08-24 04:49:07.357	31.213459895575	80.3364973889388	81.3885334594727	8.03364973889388	Heavy Rain	
7	Weather	2017-08-24 04:49:42.220	31.9218152390971	98.045405974268	91.8467895266818	9.8045405974267	Thunderstorm Light Rain	
8	Weather	2017-08-24 04:50:07.187	25.2200538415385	30.5015960384633	51.959541626934	3.05015960384633	Fog/Mat	
9	Weather	2017-08-24 04:50:42.107	30.7091591445306	67.728978132653	73.5600973818265	6.7728978132653	Light Rain Fog/Mat	
10	Weather	2017-08-24 04:51:06.987	29.0107087199652	25.267717990652	48.9079536194484	2.5267717990652	Partly Cloudy	

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**



DataServiceSetup

- □ X

Select Installation Folder



The installer will install DataServiceSetup to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:

C:\Program Files (x86)\Default Company Name\DataServiceSetup\

Browse...

Disk Cost...

Install DataServiceSetup for yourself, or for anyone who uses this computer:

Everyone

Just me

Cancel

< Back

Next >

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

Installation Incomplete



The installer was interrupted before DataServiceSetup could be installed. You need to restart the installer to try again.

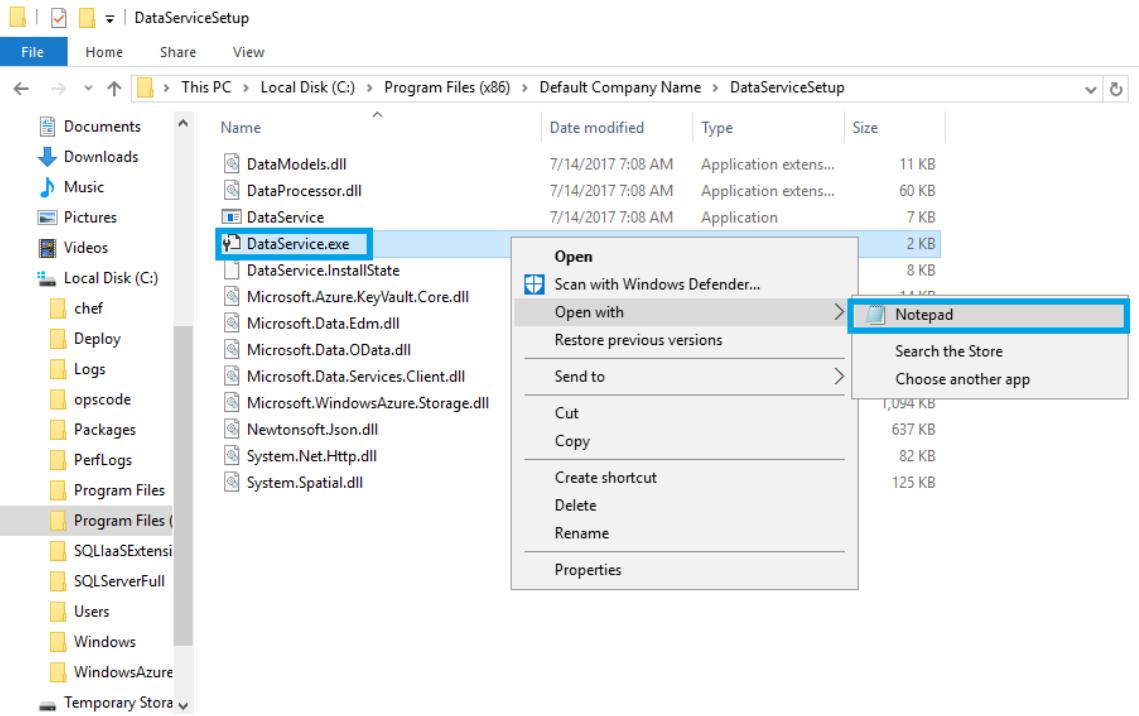
Click "Close" to exit.

Cancel

< Back

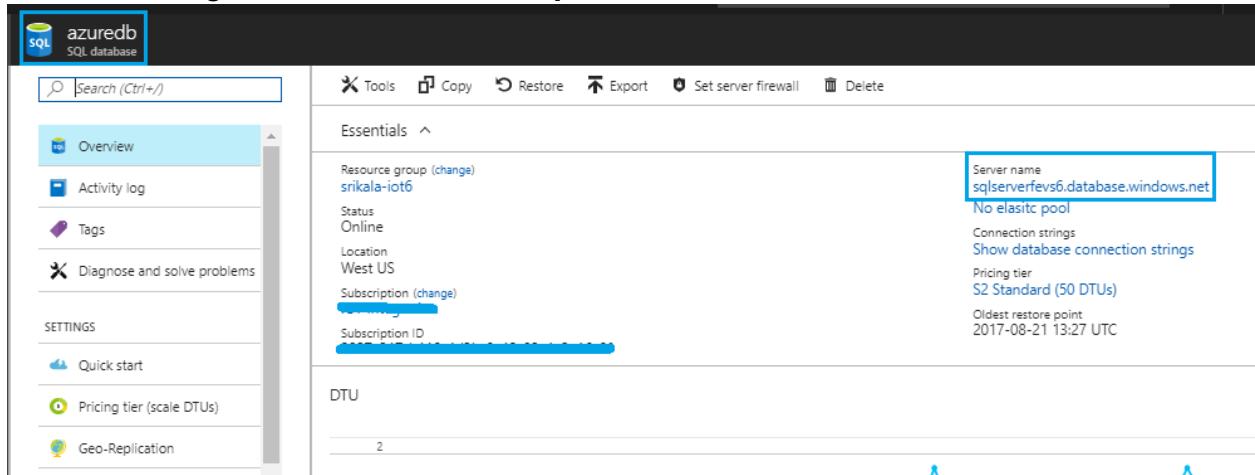
Close

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.



- 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**

+ Add **Columns** **Delete** **Refresh** **Move**

Essentials ^

Subscription name (change)
PIAF Integration

Deployments
12 Succeeded

Subscription ID
XXXXXXXXXXXXXX

Filter by name... All types All locations Group by type

77 items

NAME	TYPE	LOCATION	...
myjob4c/xn	Scheduler Job Collection	West US	...
azuredb	SQL database	West US	...
dsm	SQL database	West US	...
sqlserver4c7xh	SQL server	West US	...

webjobstr4c7xh - Access keys

Storage account

Search (Ctrl+F)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

SETTINGS

- Access keys
- Configuration

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more

Storage account name: webjobstr4c7xh

Default keys

NAME	KEY	CONNECTION STRING
key1	m92PqGkGaho8fJIAob8rXJbMifrw/5g/JfjaMQWkh...	DefaultEndpointsProtocol=https;AccountName=web...
key2	s/8MCu6Ofj6d2/SisuBacyAAdy+LeitDB39fa9Vkoz...	DefaultEndpointsProtocol=https;AccountName=web...

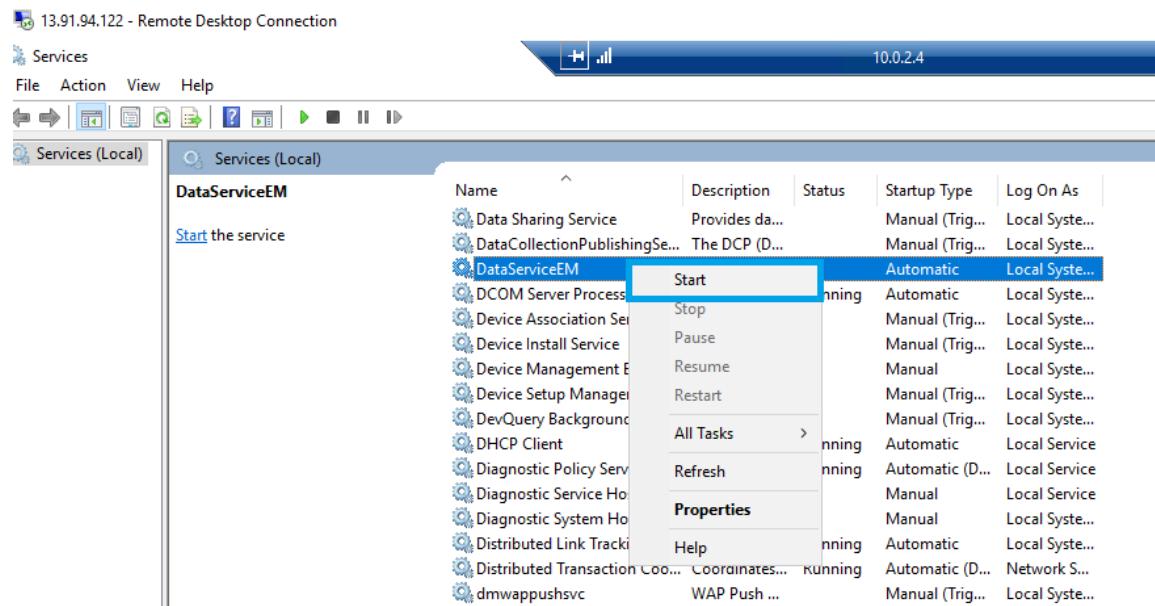
Pi Connection String: Set the **data source** as the AF server name **PIAFSQLServer**, **Initial catalog** as created database name in PIAF server which you created in PI system explorer, and the id/password as the ones used to login the SQLServer Management studio.

```

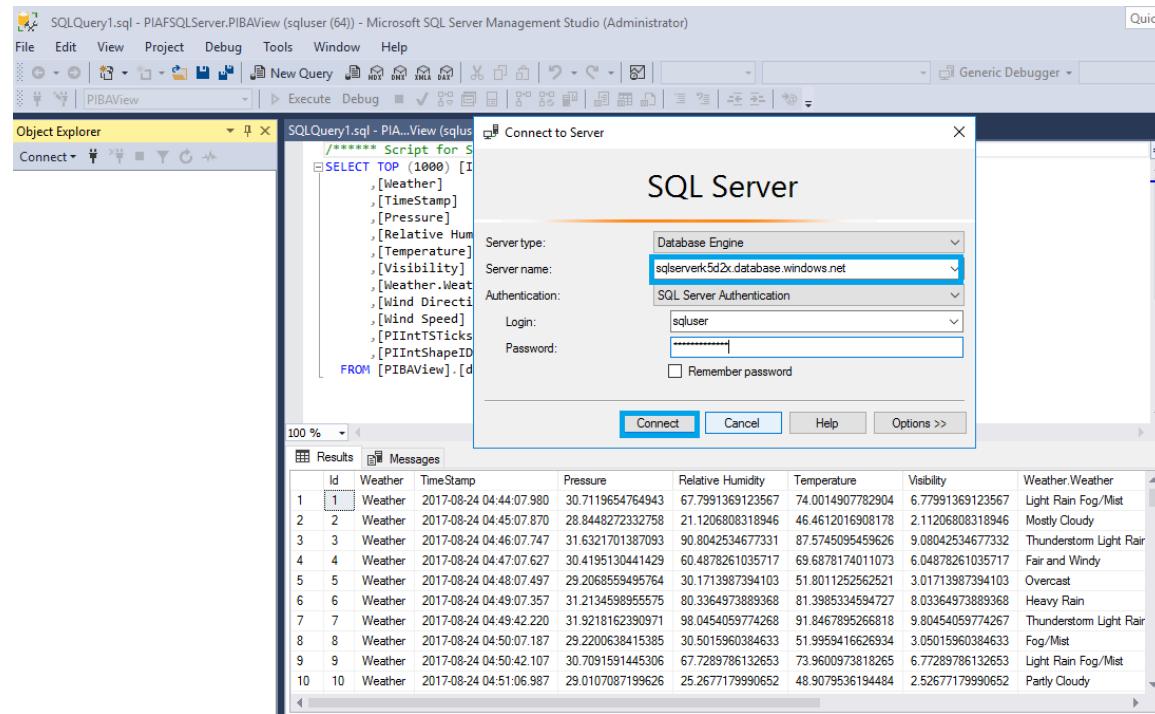
File Edit Format View Help
<xml version="1.0" encoding="utf-8">
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <appSettings>
    <add key="PIAServer" value="PIAServer1" />
    <add key="AzureConnectionString" value="Server=tcp:sqlserver4c7xh.database.windows.net,1433;Initial Catalog=azuredb;Persist Security Info=False;User ID=sqlluser;P<!-->
    <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=webjobstr4c7xh;AccountKey=m92PqGkGaho8fJIAob8rXJbMifrw/5g/JfjaMQWkh2<!-->
    <add key="PIAServerConnectionString" value="data source=PIAFSQLServer;initial catalog=PIAView;persist security info=True;user id=sqlluser;password=Password@1234" />
  </appSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6a6eed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0-10.0.0.0" newVersion="10.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>

```

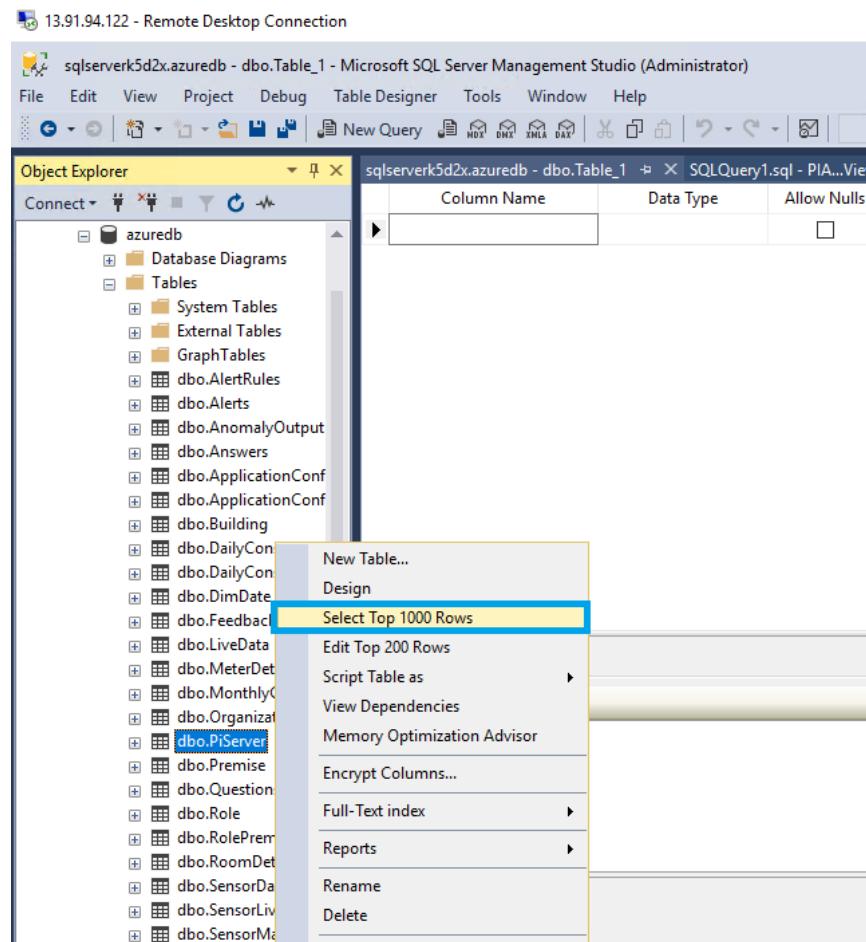
6. After updating the values in the data service.exe files, navigate **Start > Service** to start the **DataServicesEM**.



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.

13.91.94.122 - Remote Desktop Connection

SQLQuery2.sql - sqlserver5d2x.database.windows.net.azuredb (sqluser (120)) - Microsoft SQL Server Management Studio 10.0.2.4

File Edit View Query Project Debug Tools Window Help

azuredb Execute Debug Generic Debugger

Object Explorer

SQLQuery2.sql - sql...redb (sqluser (120)) # x sqlserver5d2x.azuredb - dbo.Table_1 SQLQuery1.sql - PIA...View (sqluser (64))

```
***** Script for SelectTopNRows command from SSMS *****
SELECT TOP (1000) [PiServerID]
    ,[PiServerName]
    ,[PiServerDesc]
    ,[PiServerURL]
    ,[IsActive]
    ,[CreatedBy]
    ,[CreatedOn]
    ,[ModifiedBy]
    ,[ModifiedOn]
    ,[IsDeleted]
    ,[UTCConversionTime]
FROM [dbo].[PiServer]
```

Results Messages

PiServerID	PiServerName	PiServerDesc	PiServerURL	IsActive	CreatedBy	CreatedOn	ModifiedOn
1	PiServer1	PiServer1	data source=PIAFSQLServerinitial catalog=PIBAVie...	1	NULL	2017-08-24 12:27:32.197	NULL

SQLQuery3.sql - sqlserver5d2x.database.windows.net.azuredb (sqluser (115)) - Microsoft SQL Server Management Studio 10.0.2.4

File Edit View Query Project Debug Tools Window Help

azuredb Execute Debug Generic Debugger

Object Explorer

SQLQuery3.sql - sql...redb (sqluser (115)) # x SQLQuery2.sql - sql...redb (sqluser (120)) sqlserver5d2x.azuredb - dbo.Table_1

```
select * from livedata
```

Results Messages

Id	AMPS_L1	AMPS_L2	AMPS_L3	AMPS_SYSTEM_AVG	Breaker_details	Breaker_Label
1	66.4125362430097	67.2014302966565	66.880755571763	66.8807392952078	New (2013) 3rd floor panel - almost empty	PP31 - 3rd Fl Elec
2	67.8519194764737	68.6579106702208	68.3302364539724	68.3301503558351	New (2013) 4th floor panel - almost empty	PP41 - 4th Fl Elec

SQLQuery3.sql - sqlserverk5d2x.database.windows.net.azuredb (sqluser (115)) - Microsoft SQL Server Management Studio

File Edit View Query Project Debug Tools Window Help

azuredb Execute Debug SQLQuery3.sql - sal...redb (saluser (115)) SQLQuery2.sql

Object Explorer

Connect azuredb

- 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

Results Messages

BuildingID	BuildingName	BuildingDesc	PremiseID
1	Science Building		NULL
2	Building 2		NULL
3	Building 1		NULL

SQLQuery3.sql - sqlserverk5d2x.database.windows.net.azuredb (sqluser (115)) - Microsoft SQL Server Management Studio

File Edit View Query Project Debug Tools Window Help

azuredb Execute Debug SQLQuery3.sql - sal...redb (saluser (115)) SQLQuery2.sql - sql...redb (sa)

Object Explorer

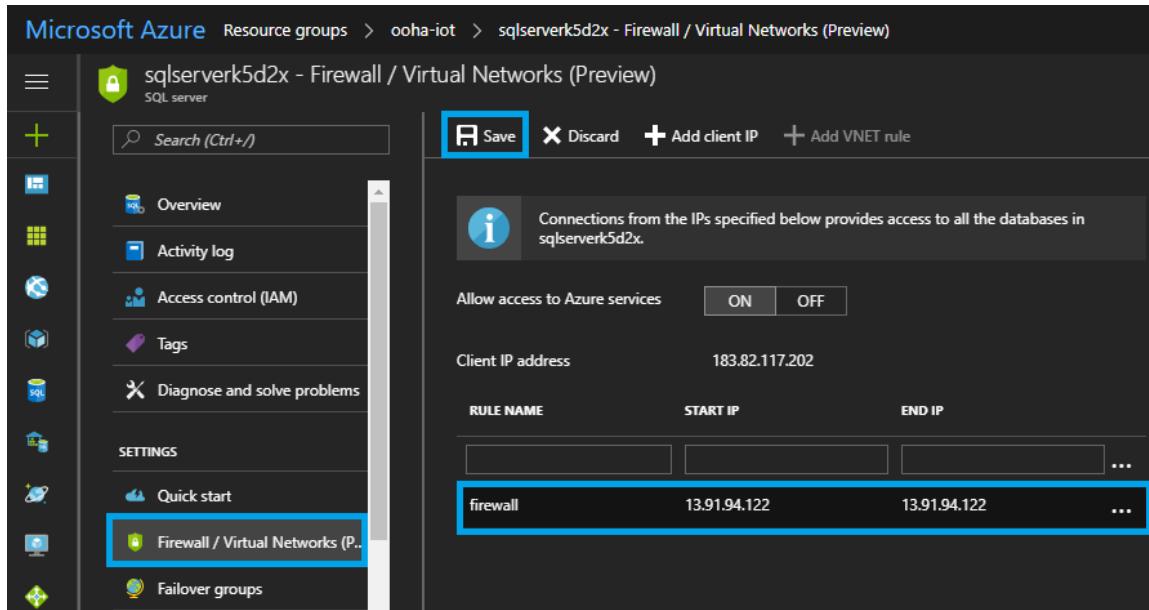
Connect azuredb

- 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

Results Messages

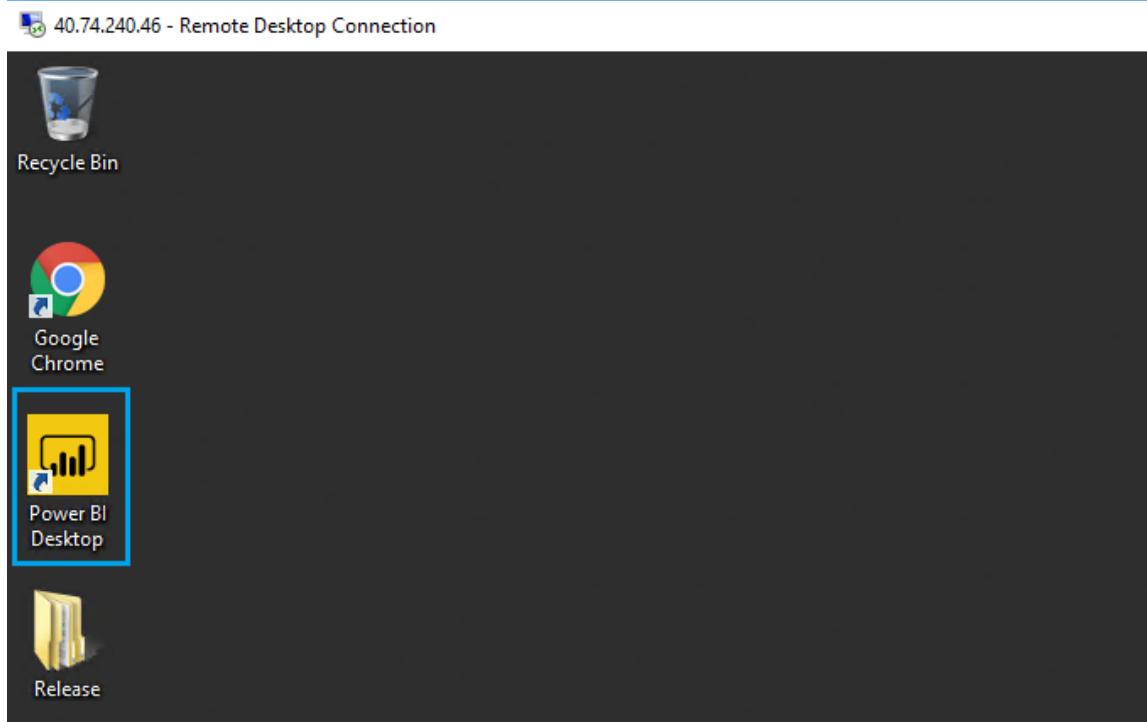
Sensor_Id	Sensor_Name	Room_Id	X	Y	PiServerName
1	Light Sensor 1	NULL	NULL	NULL	PiServer1
2	Office 1	NULL	NULL	NULL	PiServer1

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.

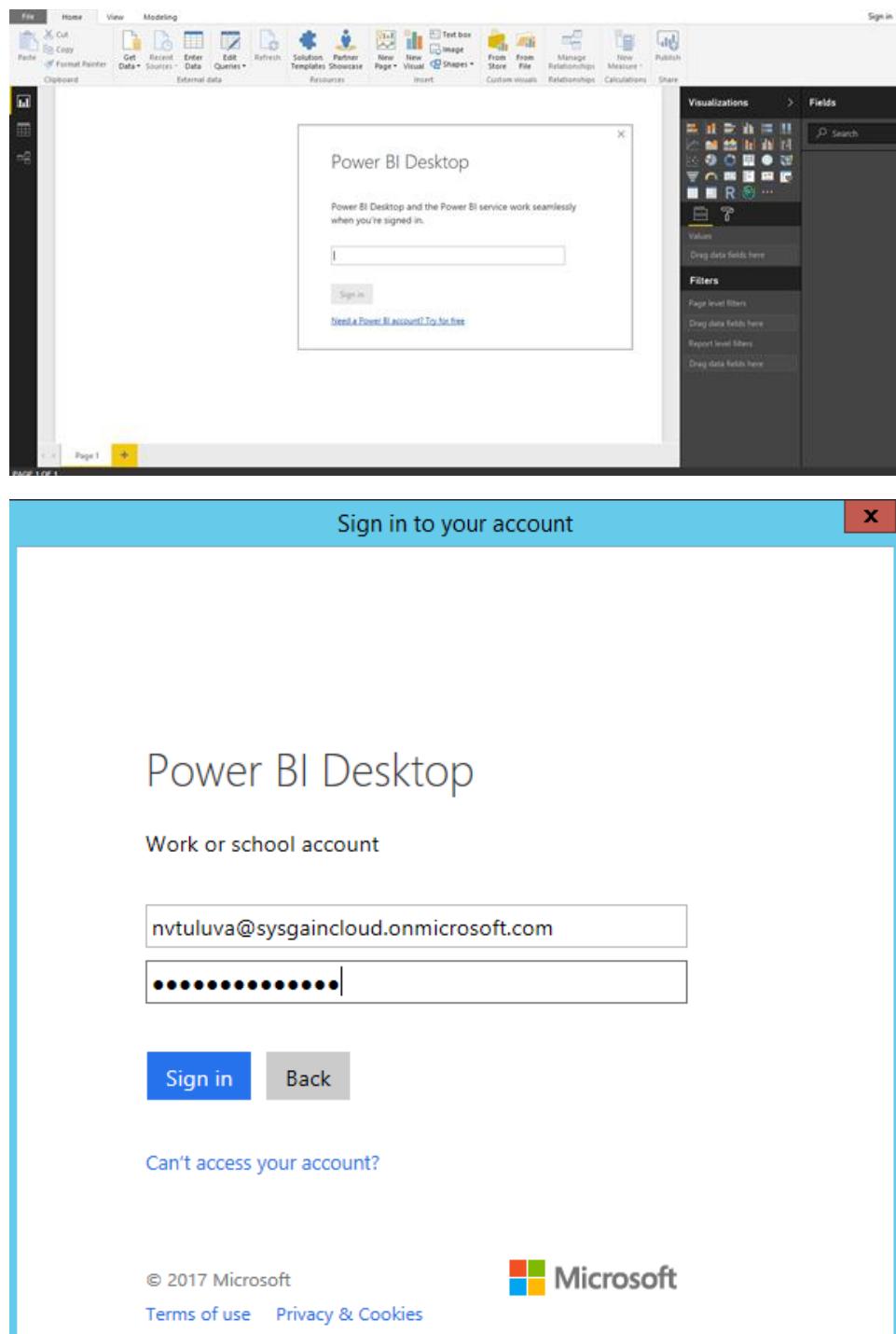


The screenshot shows the Azure portal interface for managing a SQL Server instance's firewall settings. The left sidebar lists various resources under 'Resource groups'. The main panel is titled 'sqlserver5d2x - Firewall / Virtual Networks (Preview)' and shows a table of firewall rules. One rule, named 'firewall' with 'START IP' 13.91.94.122 and 'END IP' 13.91.94.122, is selected and highlighted with a blue border. Other columns in the table include 'RULE NAME', 'START IP', 'END IP', and an ellipsis (...).

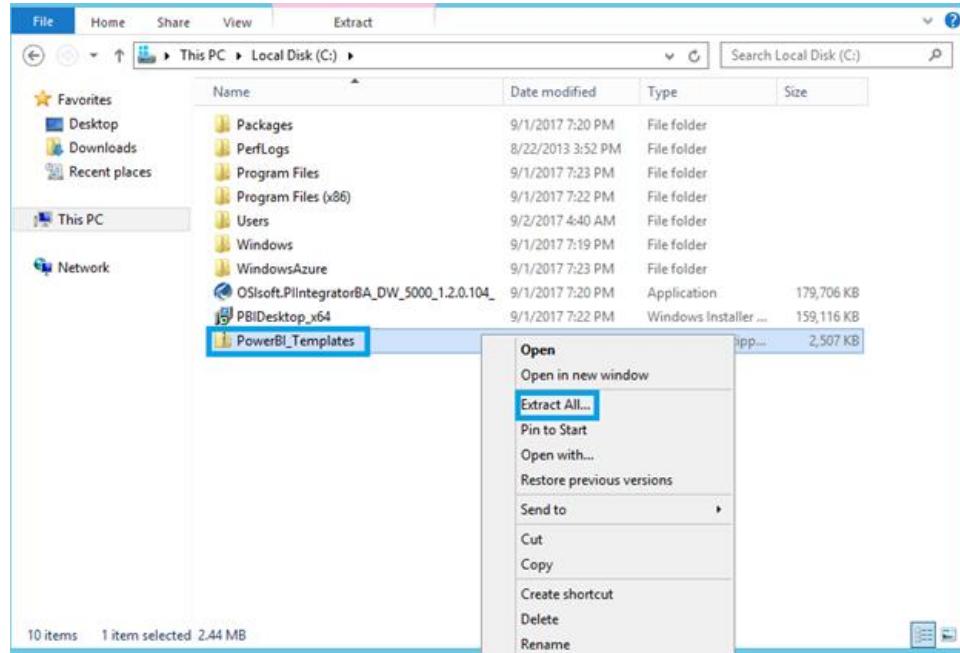
11. Login to the Bastionserver you can see the power BI desktop in Bastionserver desktop, Click on that Power BI desktop.



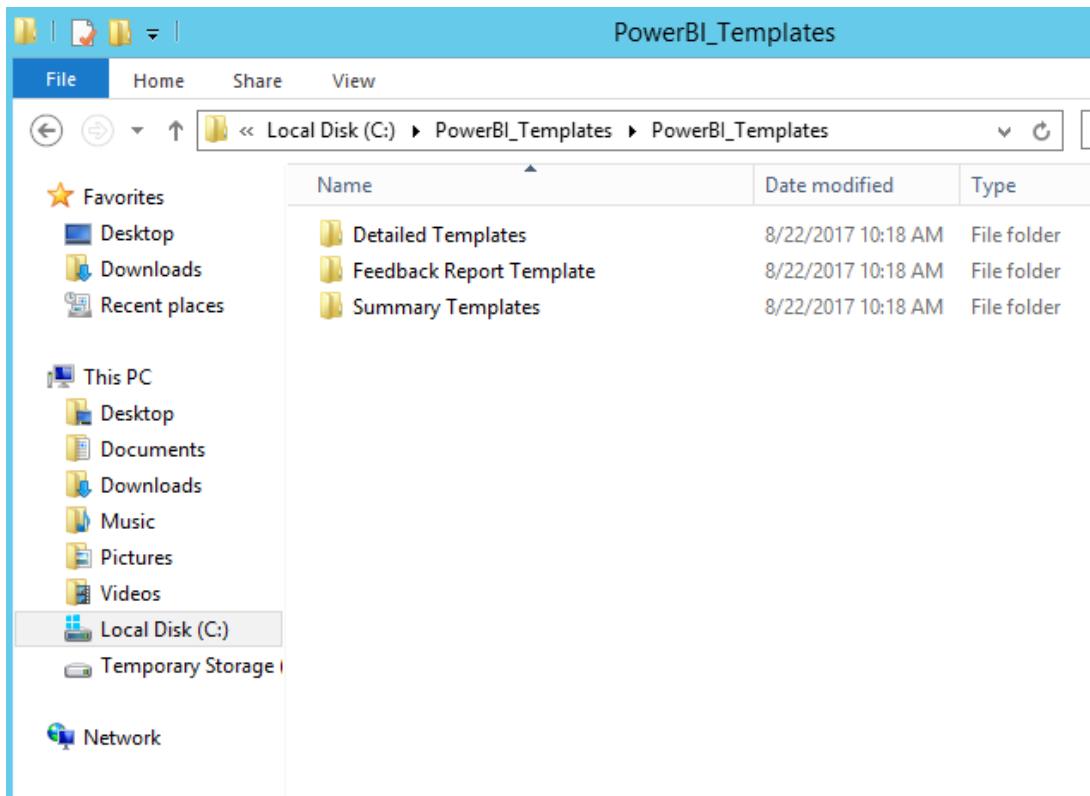
12. Log in with the same credentials used while registration of webapp with power BI you don't need to create a power BI account.



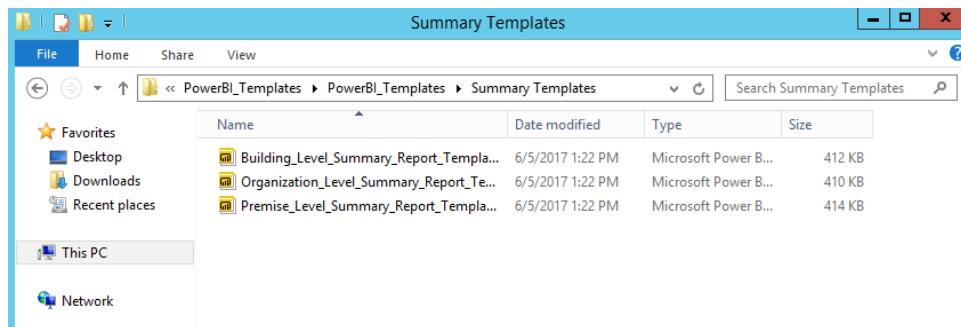
13. In Bastion server, navigate to **Local disk (C:) > unzip the Power BI templates > Power BI templates.**



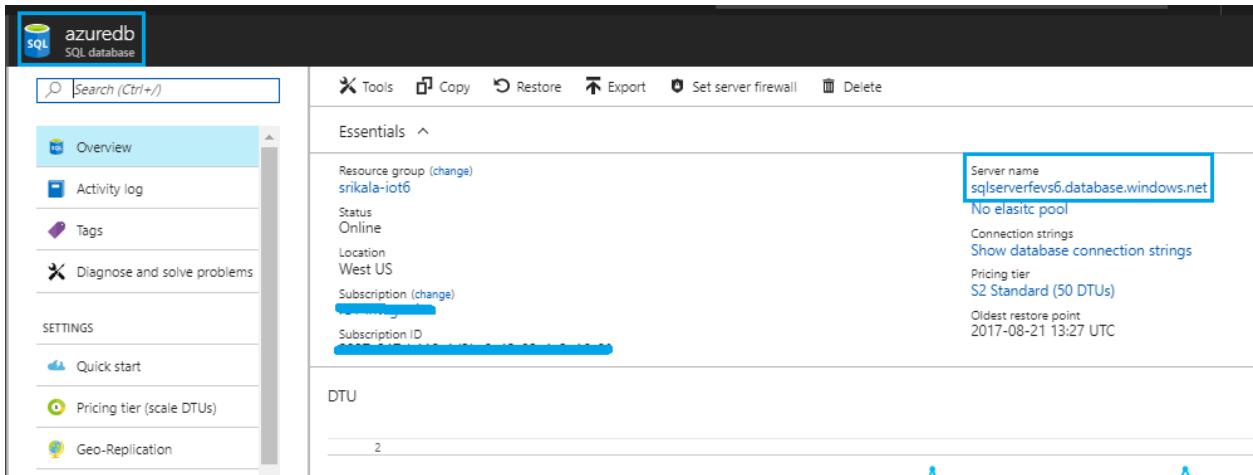
14. You can view Power BI templates in the Local disk (C:)



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



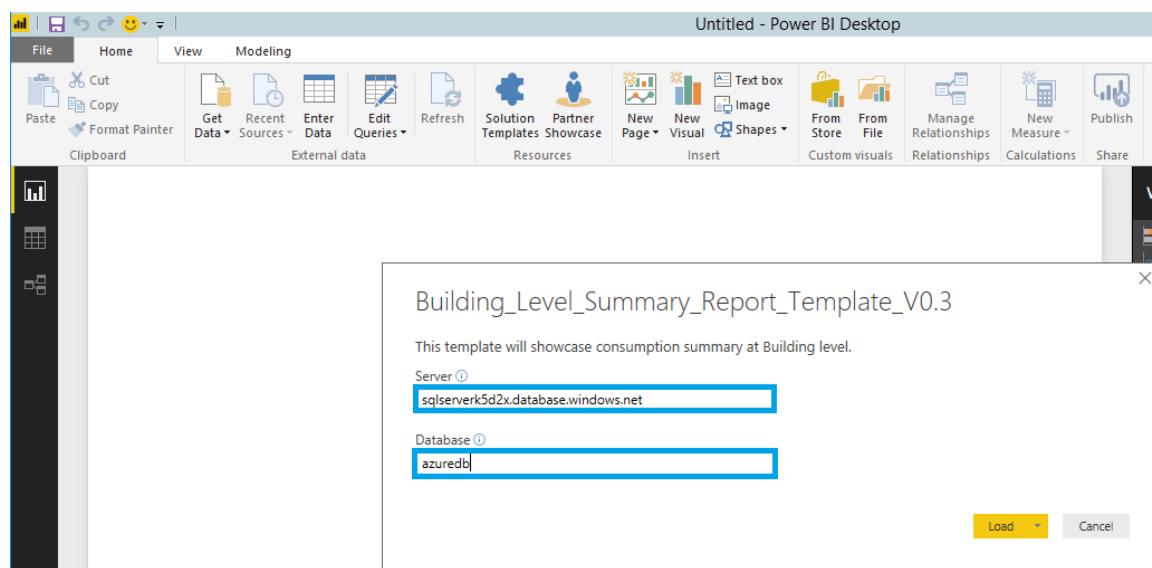
16. It prompts for power BI server and database details, provide you're Azure SQL server name and azure SQL database name from your deployed azure SQLServer .and click on **Load**.



The screenshot shows the Azure portal interface for the 'azuredb' database. The top navigation bar includes 'Tools', 'Copy', 'Restore', 'Export', 'Set server firewall', and 'Delete'. Below this, the 'Essentials' section displays the following information:

- Resource group: [srivela-iot6](#)
- Status: Online
- Location: West US
- Subscription: [\[Subscription\]](#)
- Subscription ID: [Subscription ID]
- Server name: **sqlserverfevs6.database.windows.net**
- No elastic pool
- Connection strings: [Show database connection strings](#)
- Pricing tier: **S2 Standard (50 DTUs)**
- Oldest restore point: 2017-08-21 13:27 UTC

The left sidebar contains links for Overview, Activity log, Tags, Diagnose and solve problems, SETTINGS, Quick start, Pricing tier (scale DTUs), and Geo-Replication.



The screenshot shows the Power BI Desktop interface with the title bar 'Untitled - Power BI Desktop'. The ribbon menu includes File, Home, View, and Modeling. The Home tab is selected, showing various data import and visualization tools. A dialog box is open in the center of the screen with the title 'Building_Level_Summary_Report_Template_V0.3'. It contains the following text:

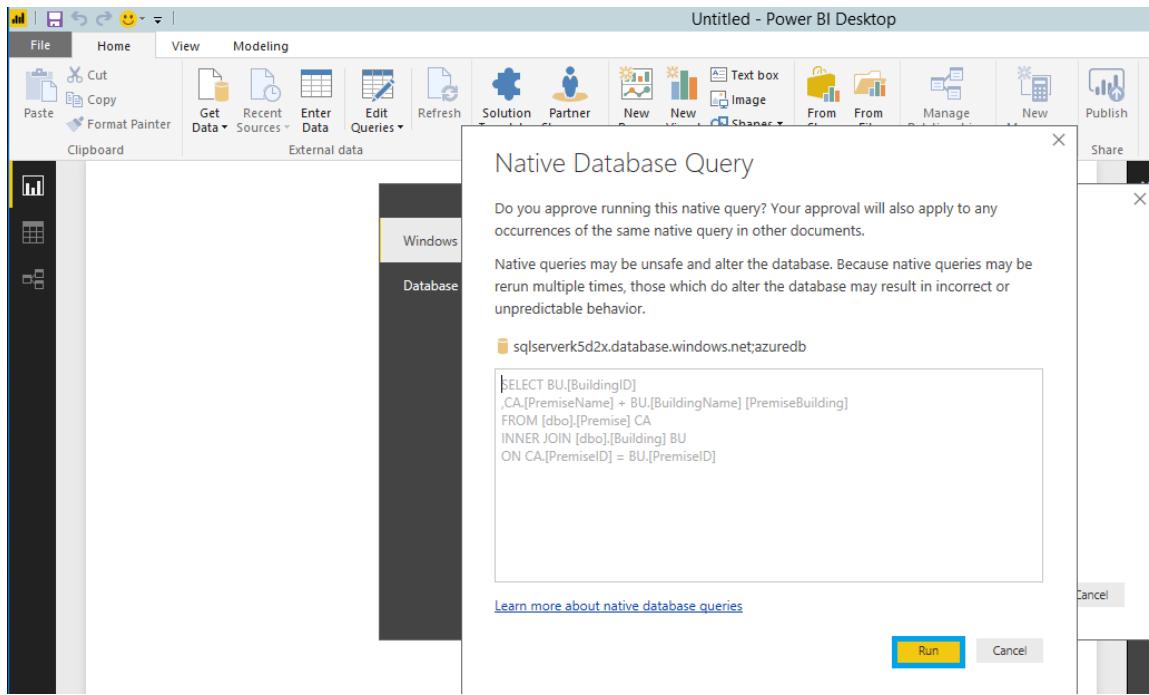
This template will showcase consumption summary at Building level.

Server: **sqlserverfevs6.database.windows.net**

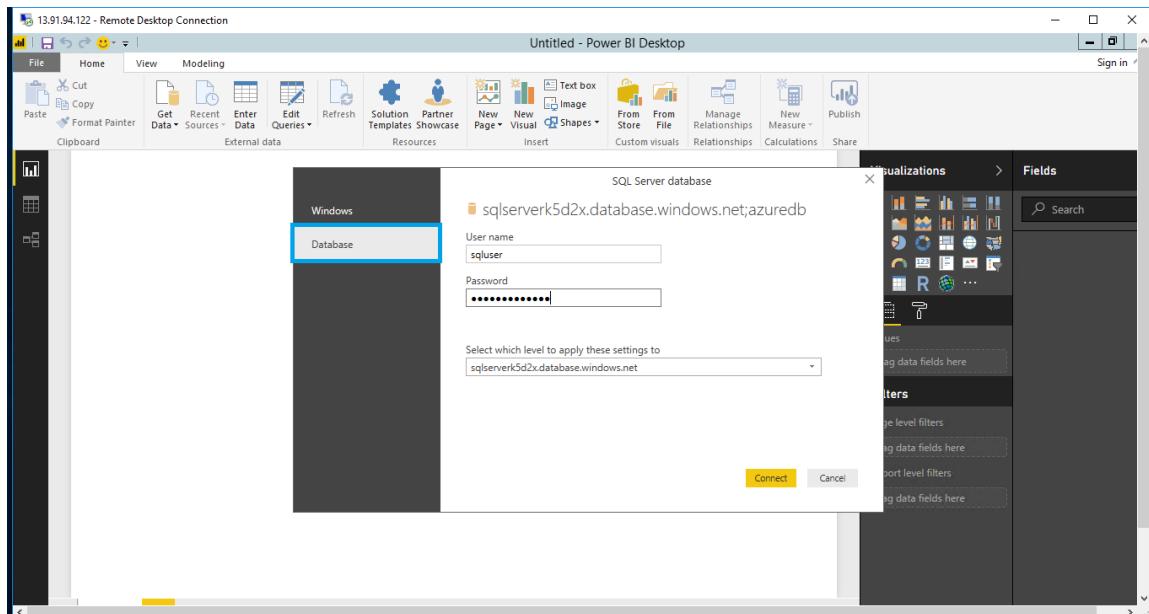
Database: **azuredb**

At the bottom right of the dialog are 'Load' and 'Cancel' buttons.

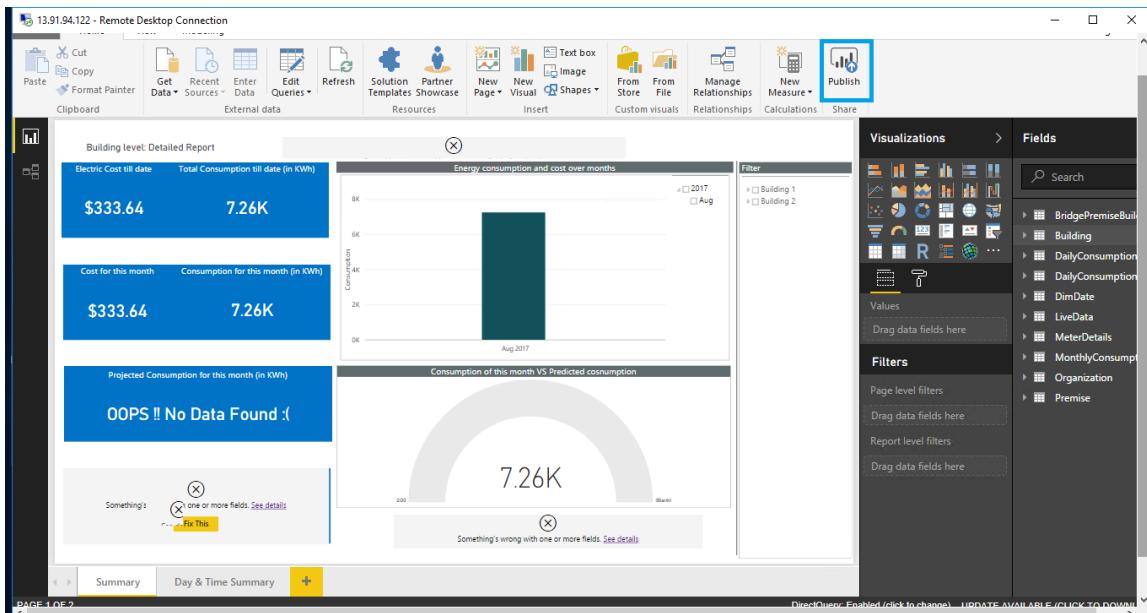
17. Once you click on Load, the “Native Database Query” will appear, click on **Run**.



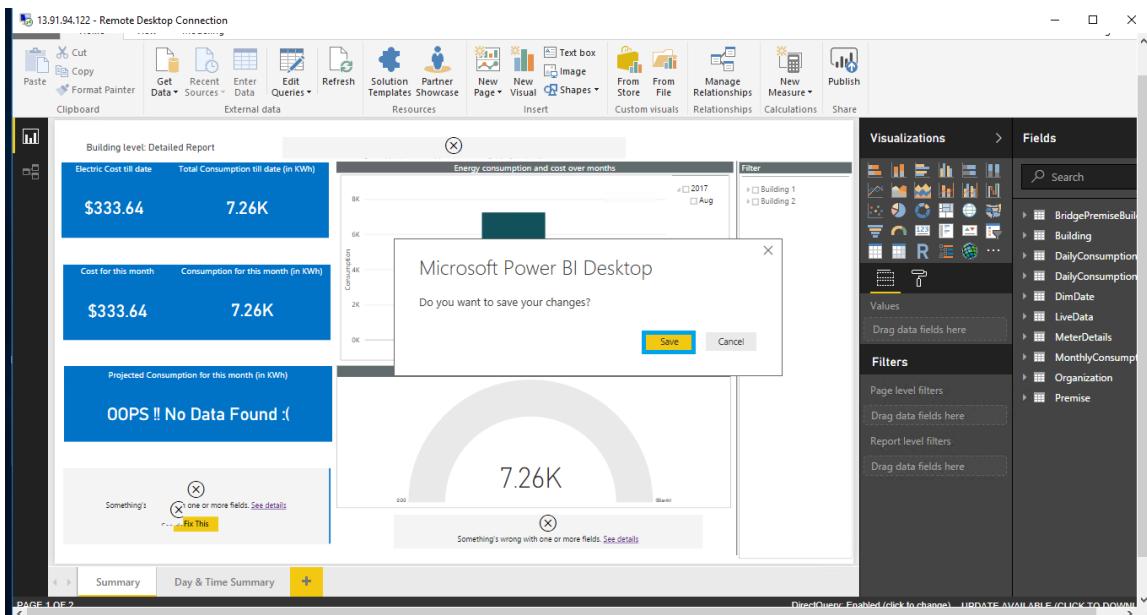
18. Select **Database** after connecting to the Azure SQL Server. Enter the login credentials of Azure database and click on **Connect**.



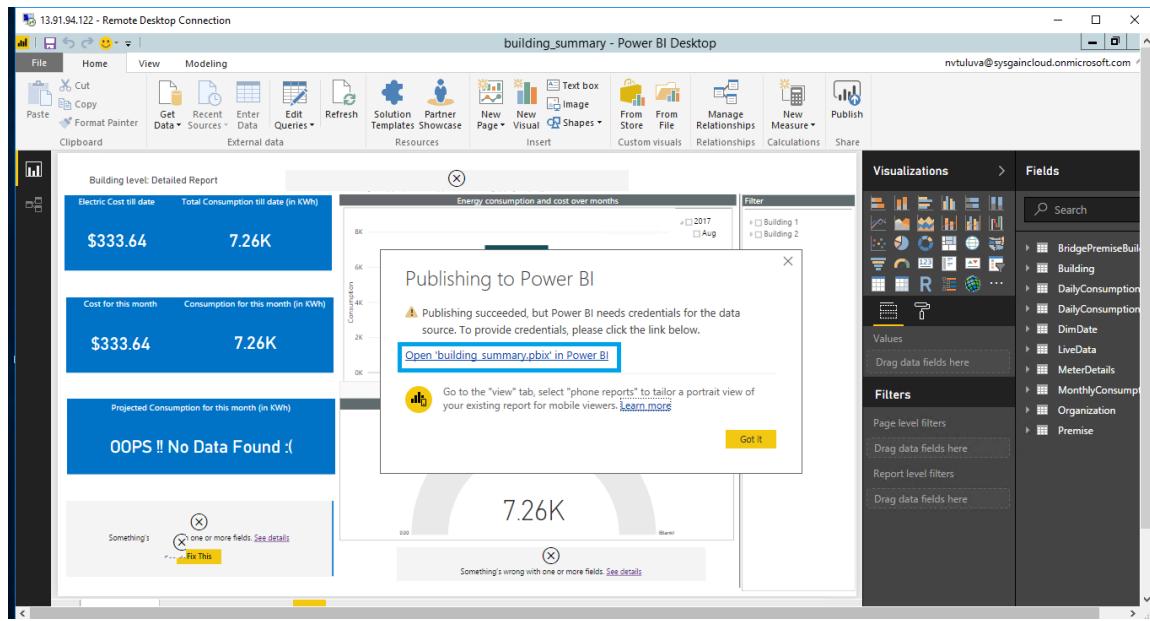
19. Click on **Publish**.



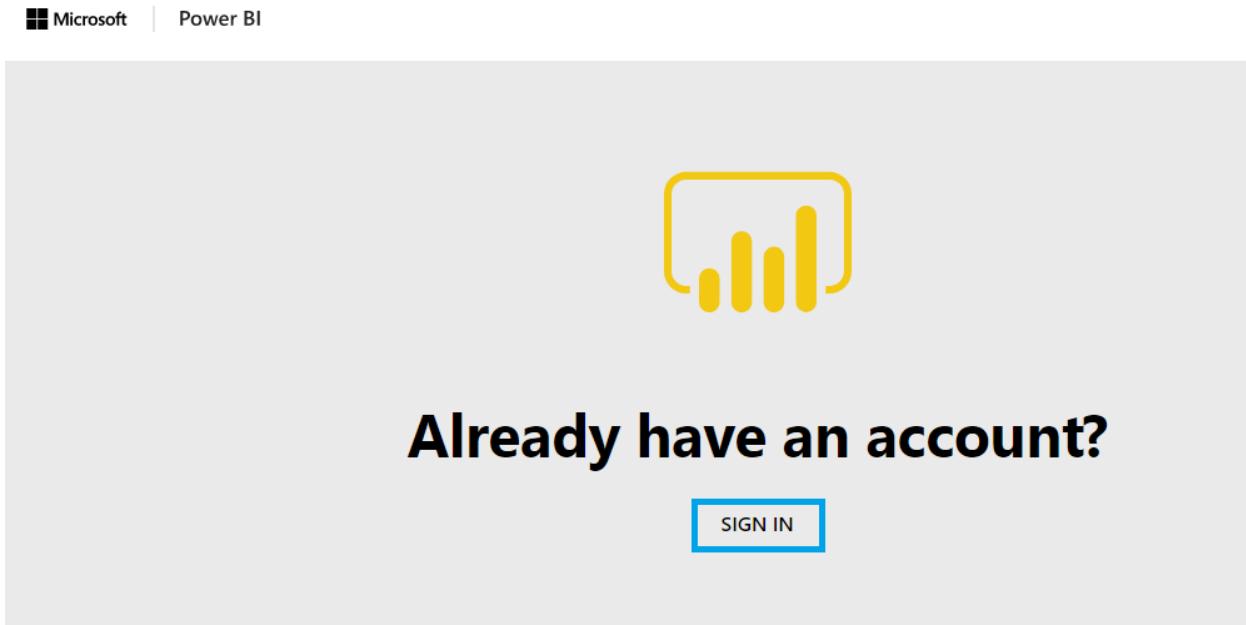
20. Save the changes.



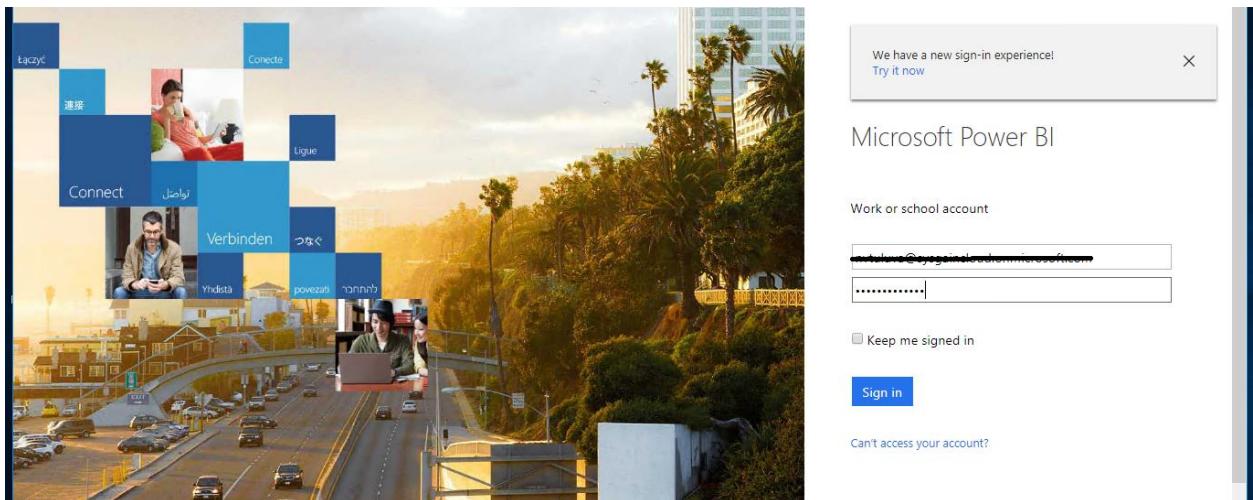
21. Click on the link as shown below, it will open in a web browser.



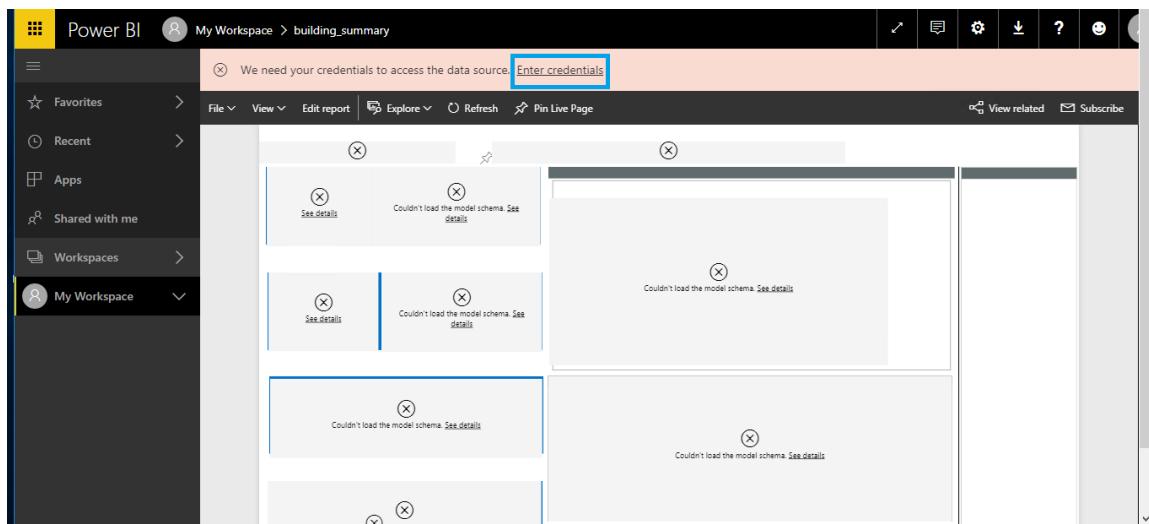
22. Sign in with the same credentials which were used to log to Power BI.



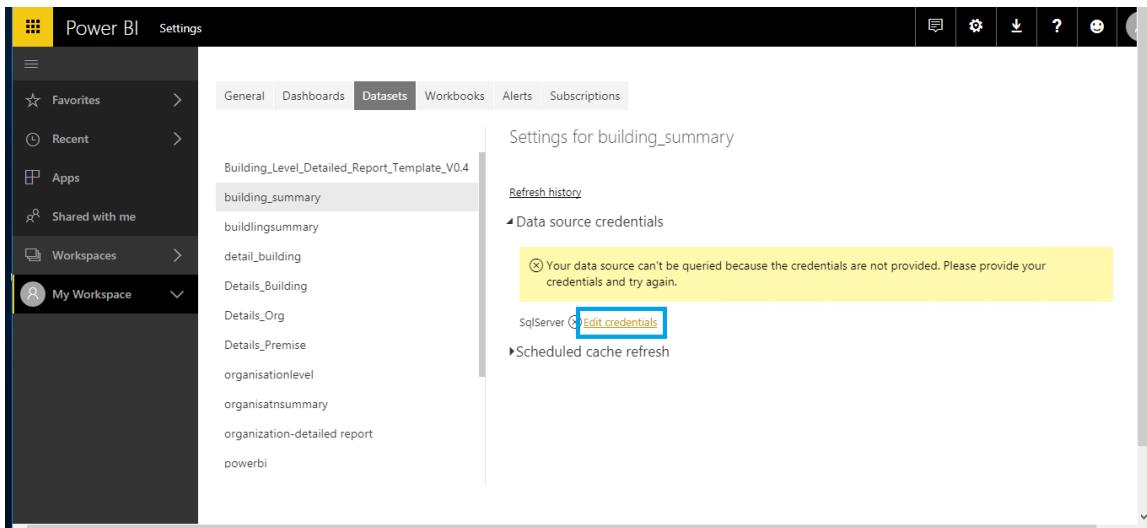
23. Enter the Power BI Credentials.



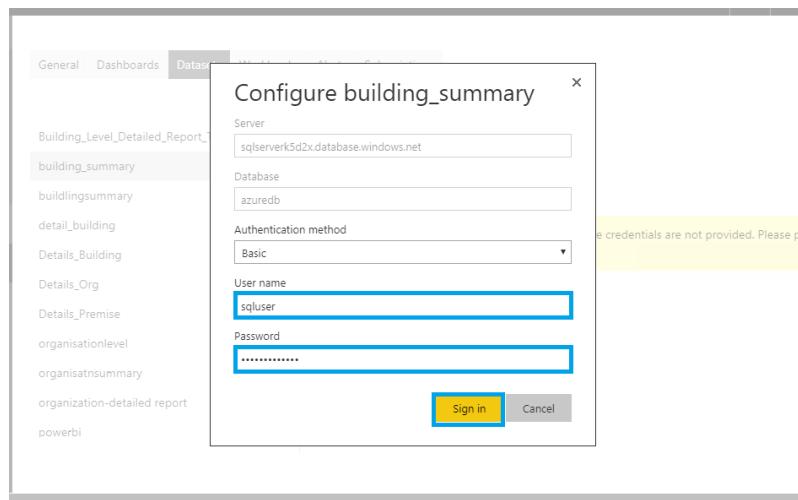
24. Click on **Enter credentials**.



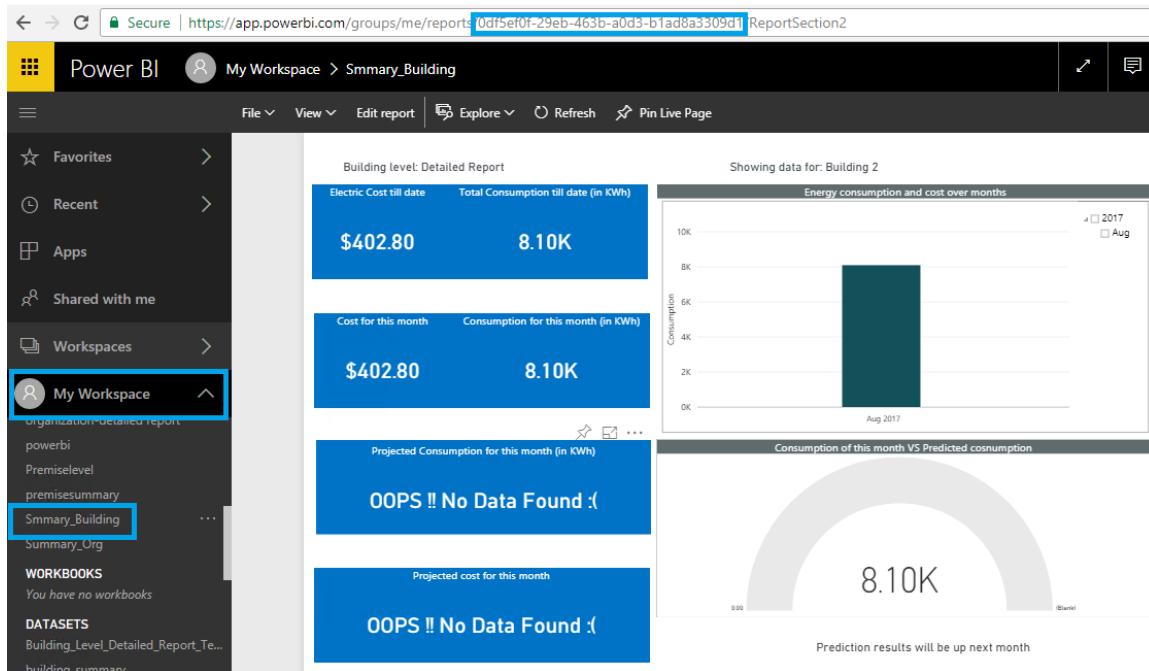
25. Click on **Edit credentials**.



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



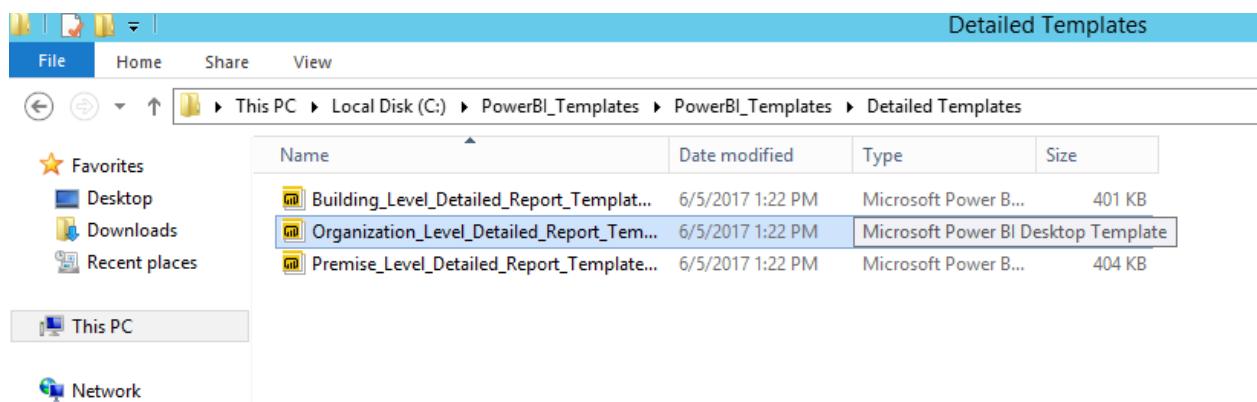
27. Copy the token from the URL publishing each template and save it for further configuration in web app.



The screenshot shows a Power BI workspace interface. On the left, the 'My Workspace' menu is open, displaying several reports and templates. One template, 'Smmry_Building', is highlighted with a blue border. The main area shows the published report titled 'Building level: Detailed Report'. It displays two key figures: 'Electric Cost till date' (\$402.80) and 'Total Consumption till date (in KWh)' (8.10K). Below these, there are sections for 'Cost for this month' and 'Consumption for this month (in KWh)', both showing the same values (\$402.80 and 8.10K). A warning message 'OOPS !! No Data Found :(' appears in two places: 'Projected Consumption for this month (in KWh)' and 'Projected cost for this month'. To the right, there is a bar chart titled 'Energy consumption and cost over months' showing consumption for August 2017, and a gauge chart titled 'Consumption of this month VS Predicted consumption' showing a value of 8.10K.

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

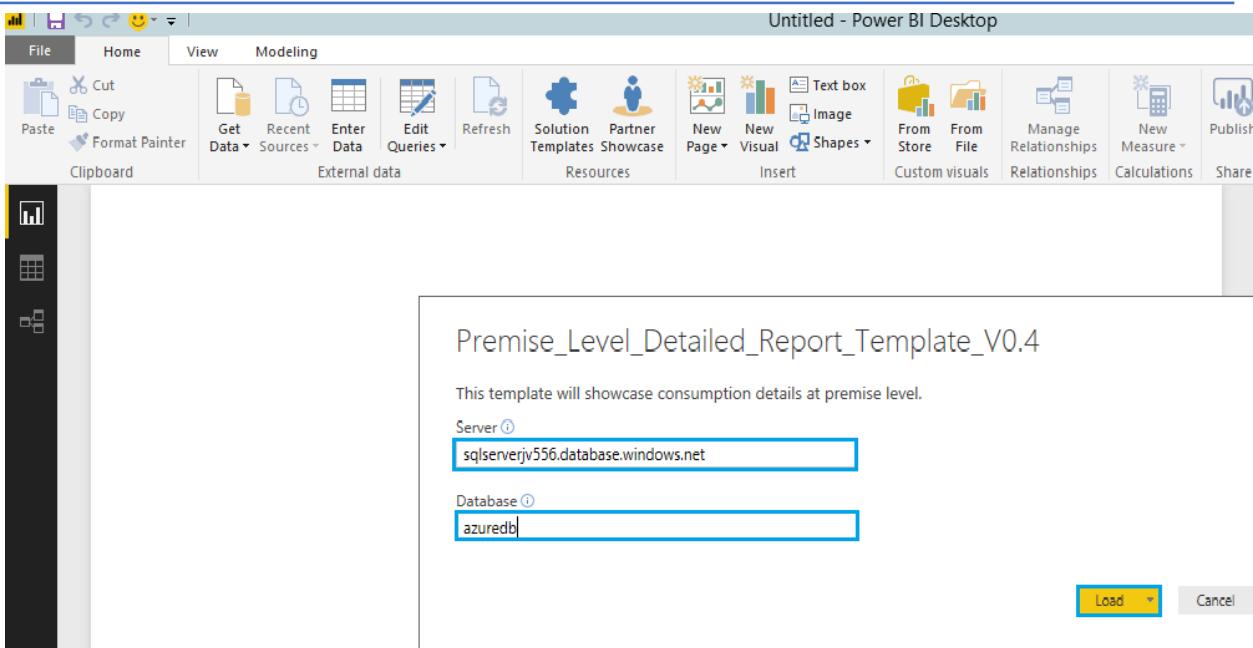
29. Navigate to **Power BI** templates and select **Detailed Template**



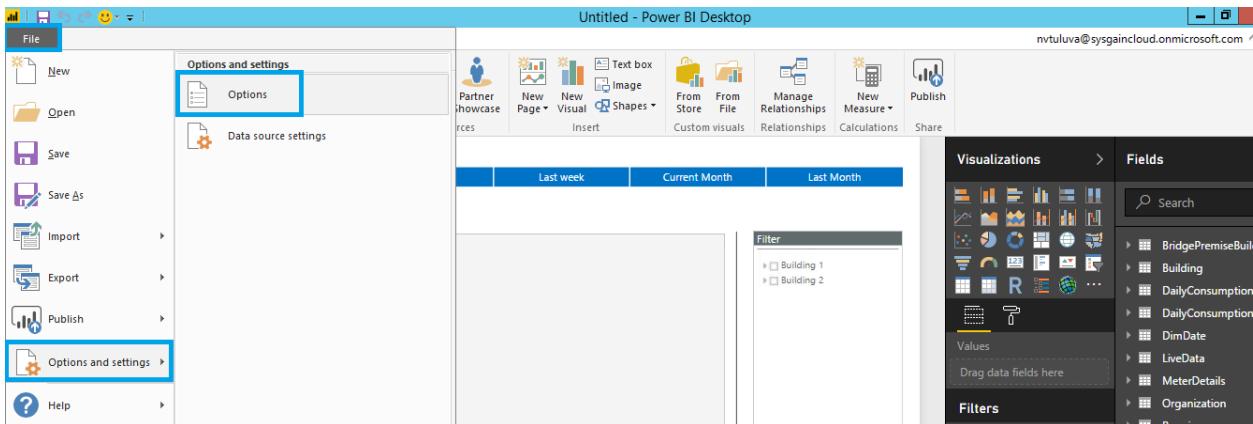
The screenshot shows a Windows File Explorer window. The title bar says 'Detailed Templates'. The address bar shows the path: This PC > Local Disk (C:) > PowerBI_Templates > PowerBI_Templates > Detailed Templates. The left sidebar shows 'Favorites' with options like Desktop, Downloads, and Recent places. The main pane lists three files in a table:

Name	Date modified	Type	Size
Building_Level_Detailed_Report_Template...	6/5/2017 1:22 PM	Microsoft Power B...	401 KB
Organization_Level_Detailed_Report_Tem...	6/5/2017 1:22 PM	Microsoft Power BI Desktop Template	
Premise_Level_Detailed_Report_Template...	6/5/2017 1:22 PM	Microsoft Power B...	404 KB

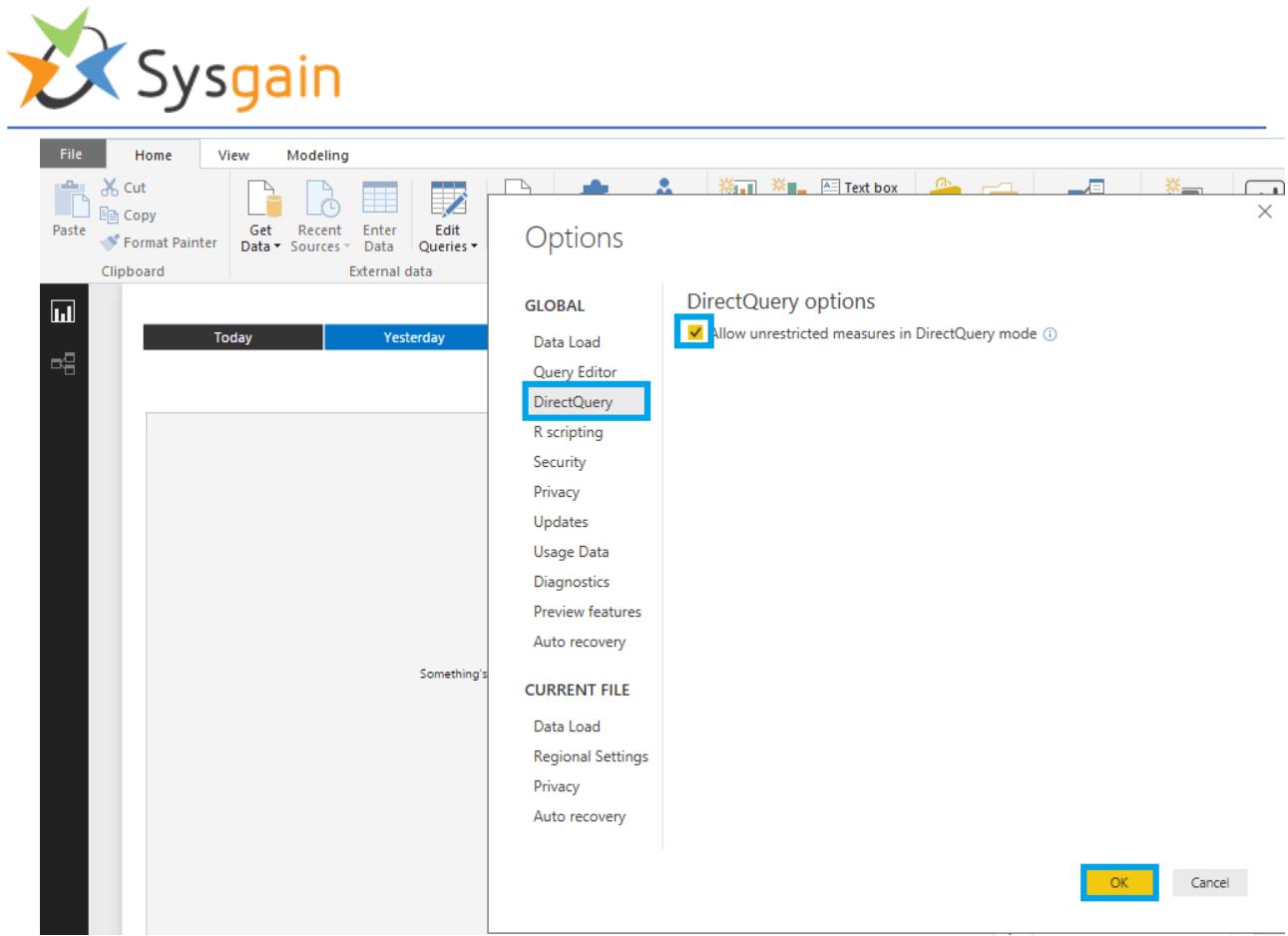
30. Enter the Azure SQL Server name with its password.



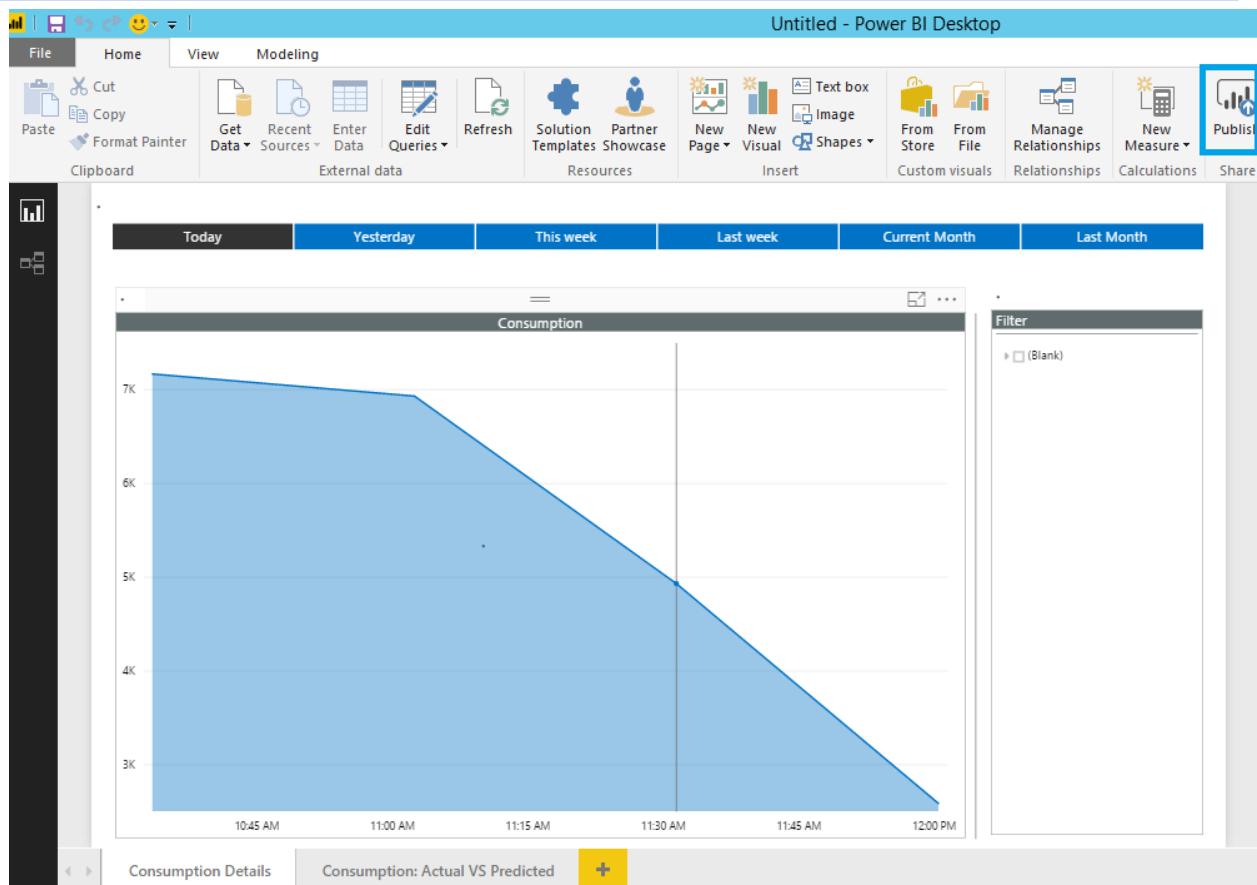
31. Navigate to **File > Options and Settings > Options**.



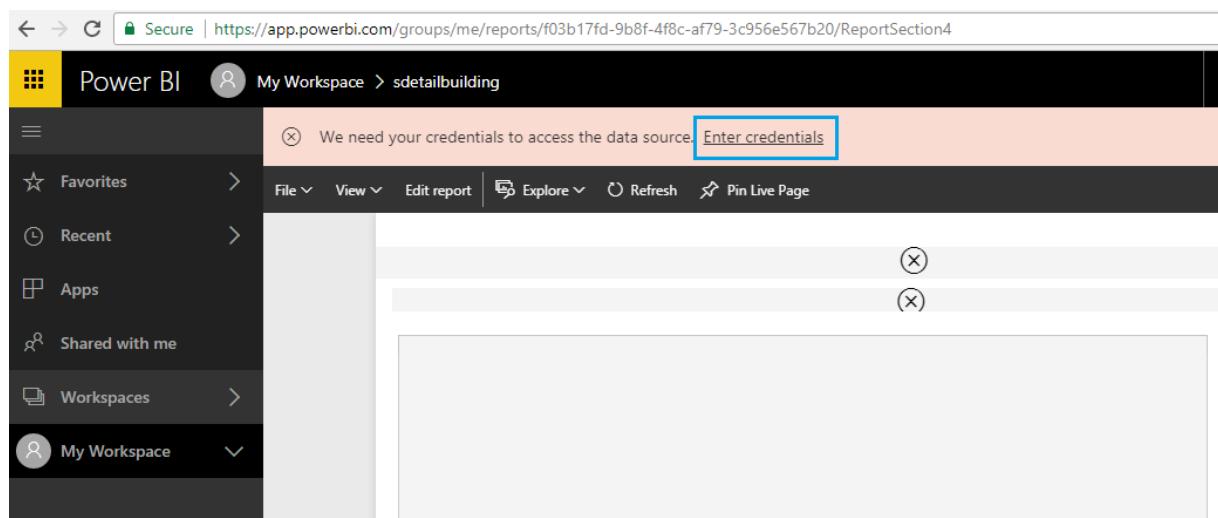
32. Select **DirectQuery** and then click on **OK**. Follow the same Process as done for the Summary template.



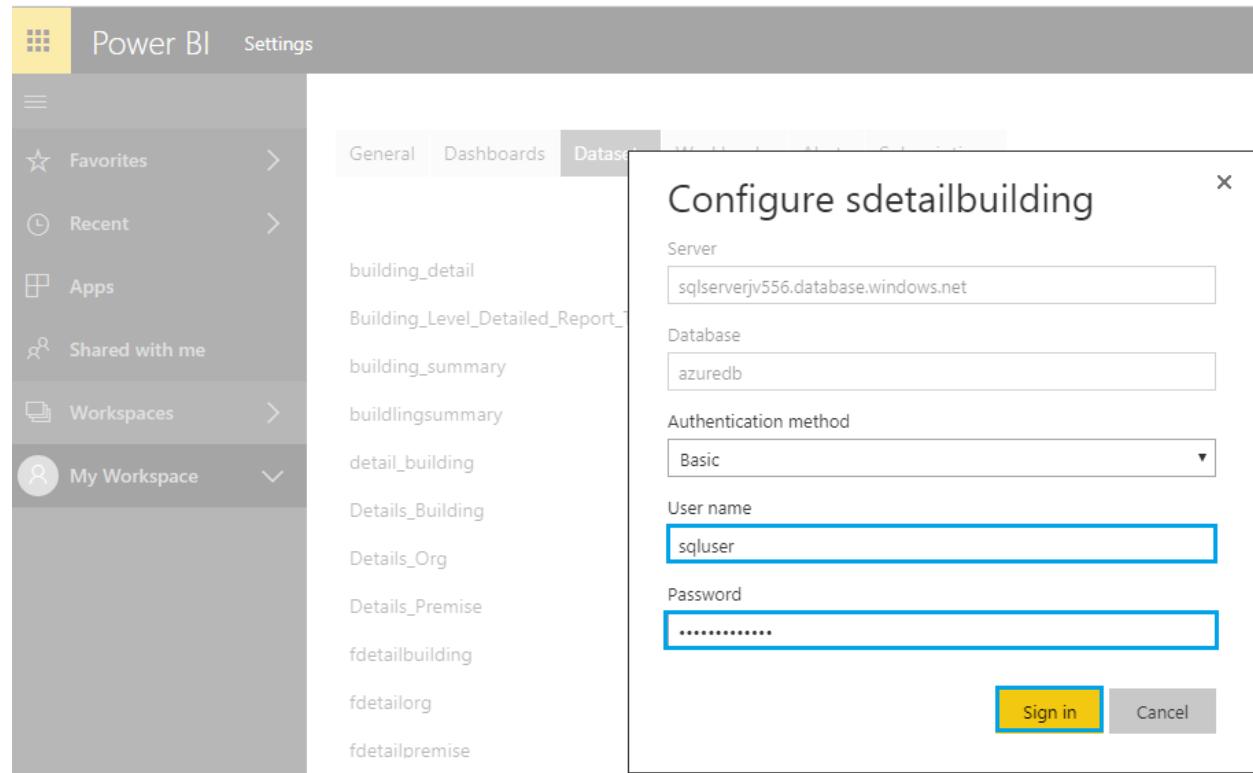
33. Click on **Publish** when you view the graph.



34. Click on **Enter credentials**.

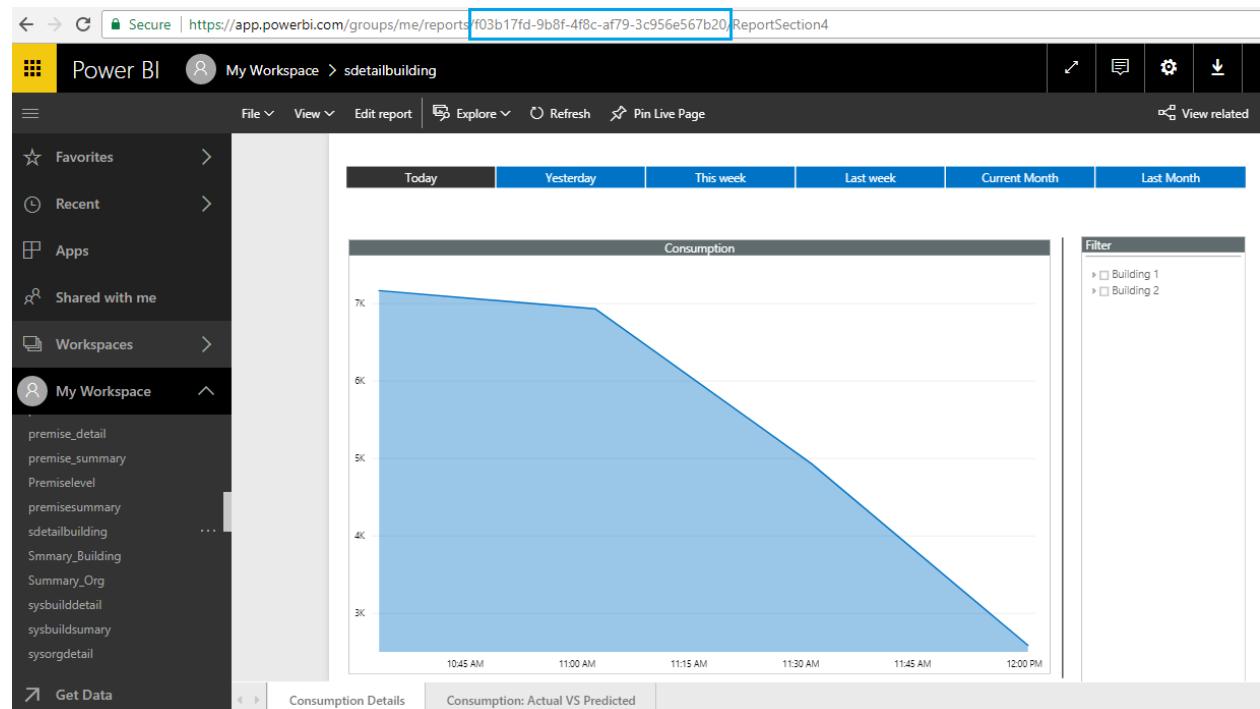


35. Enter the Azure SQL Server **User name** and **Password**.



The screenshot shows the Power BI interface. On the left, there's a navigation pane with 'Power BI' and 'Settings' at the top, followed by 'Favorites', 'Recent', 'Apps', 'Shared with me', 'Workspaces', and 'My Workspace'. Under 'My Workspace', several reports are listed: 'building_detail', 'Building_Level_Detailed_Report...', 'building_summary', 'buildingsummary', 'detail_building', 'Details_Building', 'Details_Org', 'Details_Premise', 'fdetailbuilding', 'fdetailorg', and 'fdetailpremise'. A modal dialog box titled 'Configure sdetailbuilding' is open in the center. It contains fields for 'Server' (sqlserverjv556.database.windows.net), 'Database' (azuredb), 'Authentication method' (Basic), 'User name' (sqluser), and 'Password' (redacted). At the bottom right of the dialog are 'Sign in' and 'Cancel' buttons.

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



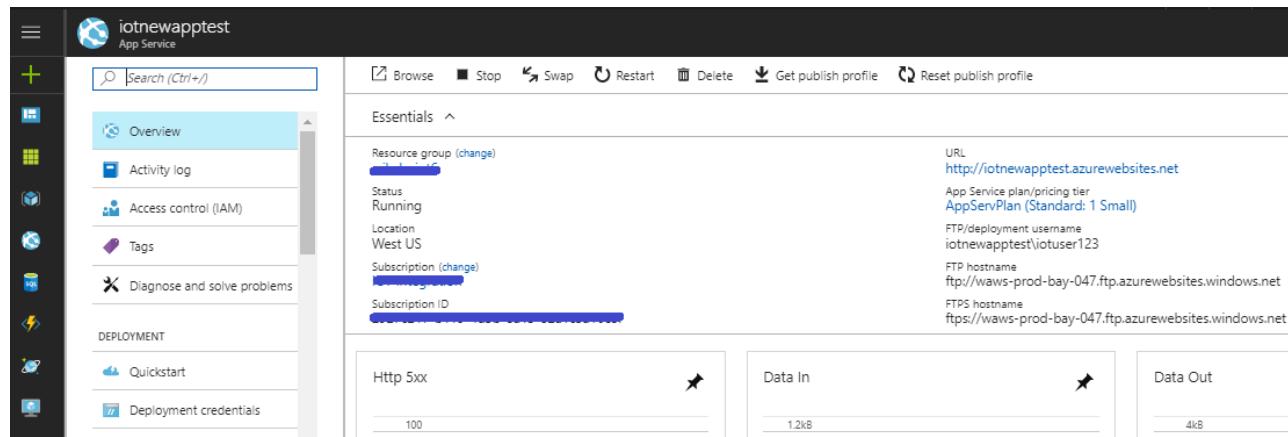
The screenshot shows the published report in the Power BI service. The URL in the browser address bar is https://app.powerbi.com/groups/me/reports/f03b17fd-9b8f-4f8c-af79-3c956e567b20/ReportSection4. The interface includes a top navigation bar with 'Secure', 'File', 'View', 'Edit report', 'Explore', 'Refresh', 'Pin Live Page', and 'View related'. Below this is a left sidebar with 'Favorites', 'Recent', 'Apps', 'Shared with me', 'Workspaces', and 'My Workspace'. Under 'My Workspace', the report 'sdetailbuilding' is selected. The main area displays a chart titled 'Consumption' showing a blue area graph of consumption levels over time, with a downward trend from approximately 7K to 3K. The x-axis shows times from 10:45 AM to 12:00 PM. A filter panel on the right shows options for 'Building 1' and 'Building 2'.

238

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 address listed under "**URL**".



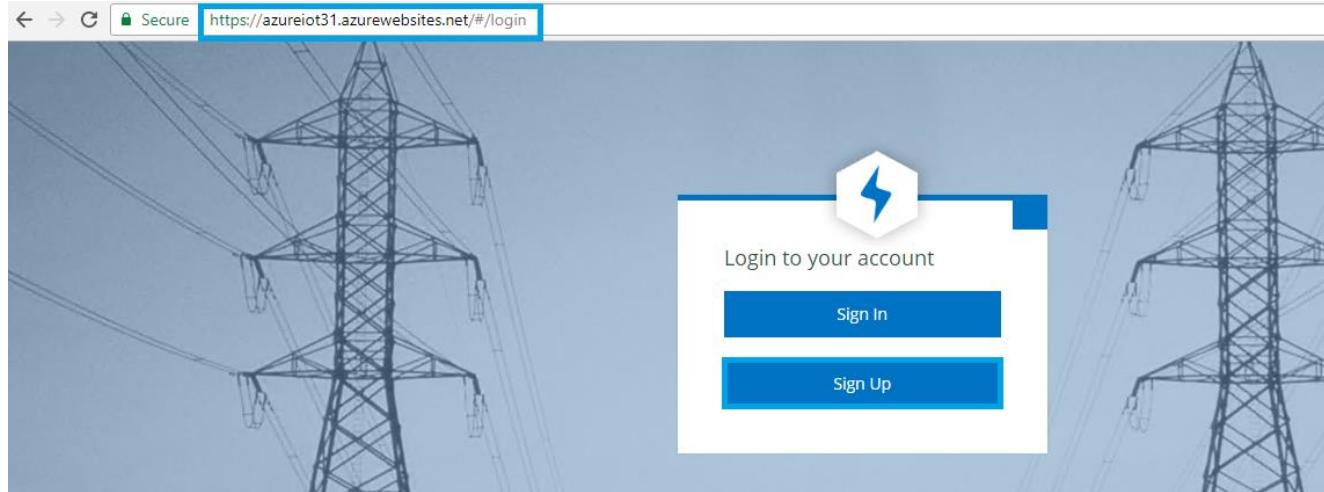
The screenshot shows the Azure portal interface for the 'iotnewapp' App Service. The left sidebar has a 'Search (Ctrl+/' input field. The main area shows the 'Overview' tab selected. The 'Essentials' section displays the following details:

Setting	Value
Resource group (change)	[REDACTED]
Status	Running
Location	West US
Subscription (change)	[REDACTED]
Subscription ID	[REDACTED]

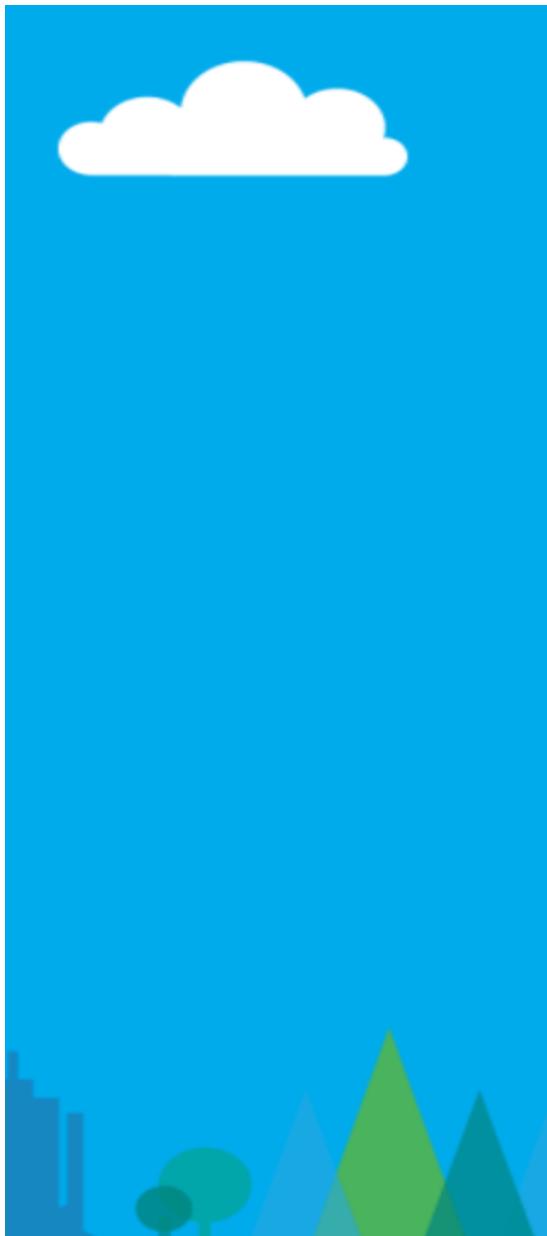
On the right, there are sections for 'Http 5xx', 'Data In', and 'Data Out' with their respective values: 100, 12kB, and 4kB. The URL is listed as:

URL
http://iotnewapp.azurewebsites.net

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

New Password

Confirm New Password

Surname

Street Address

State/Province

Postal Code

Job Title

Given Name

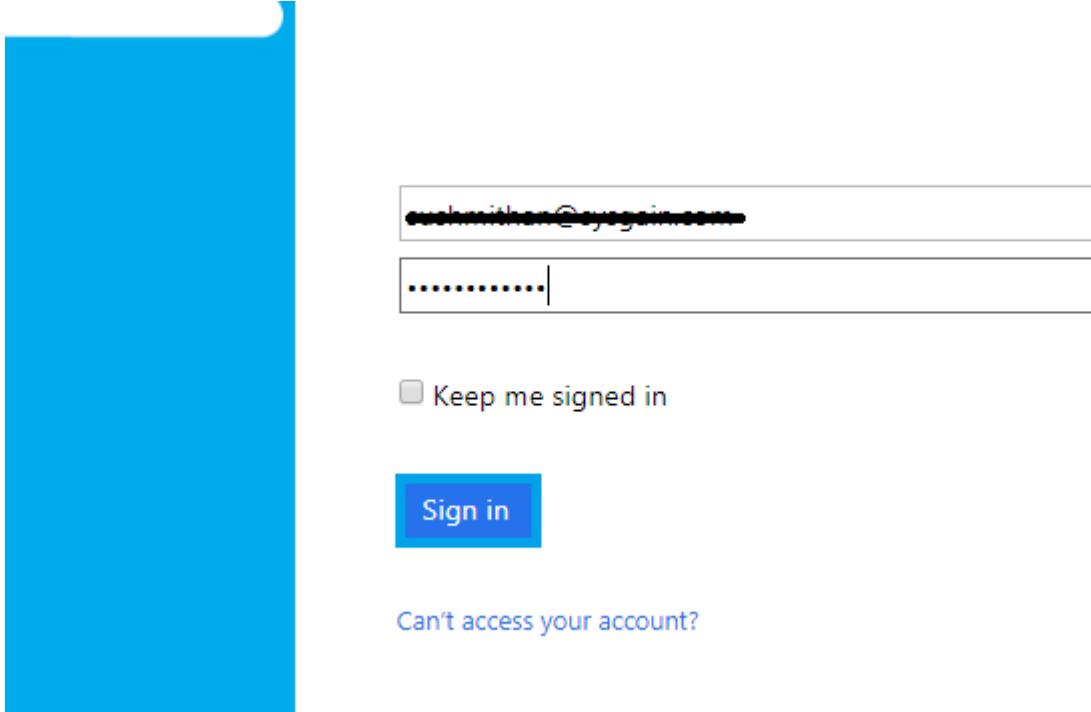
Display Name

Country/Region
 ▾

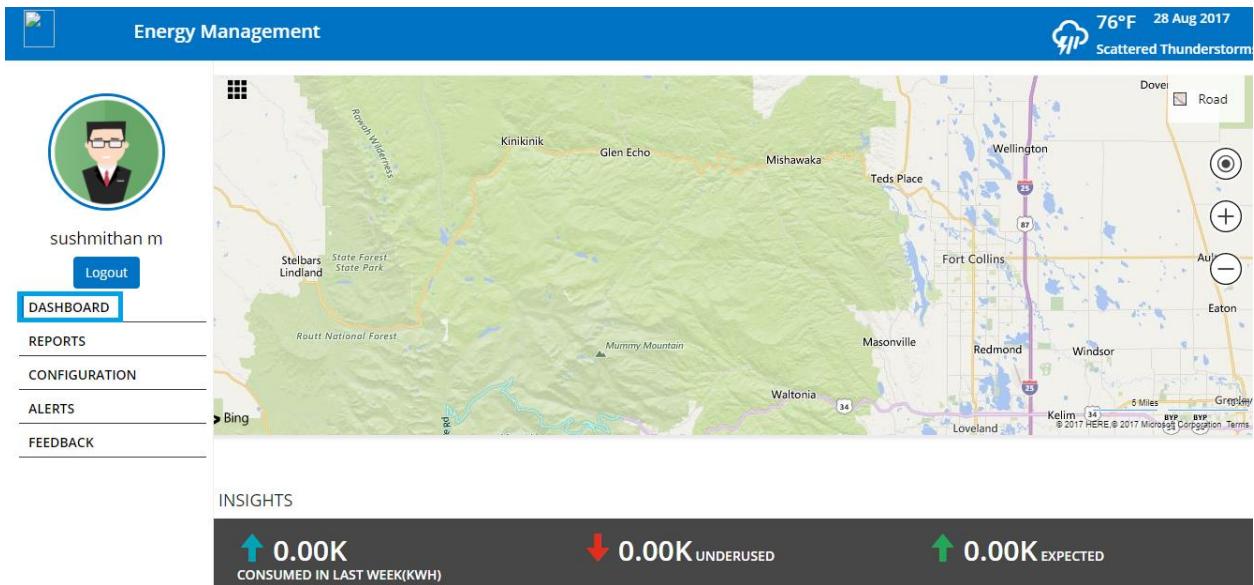
City

Activate Windows
[Get 10% off Settings to activate Windows 10](#)

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



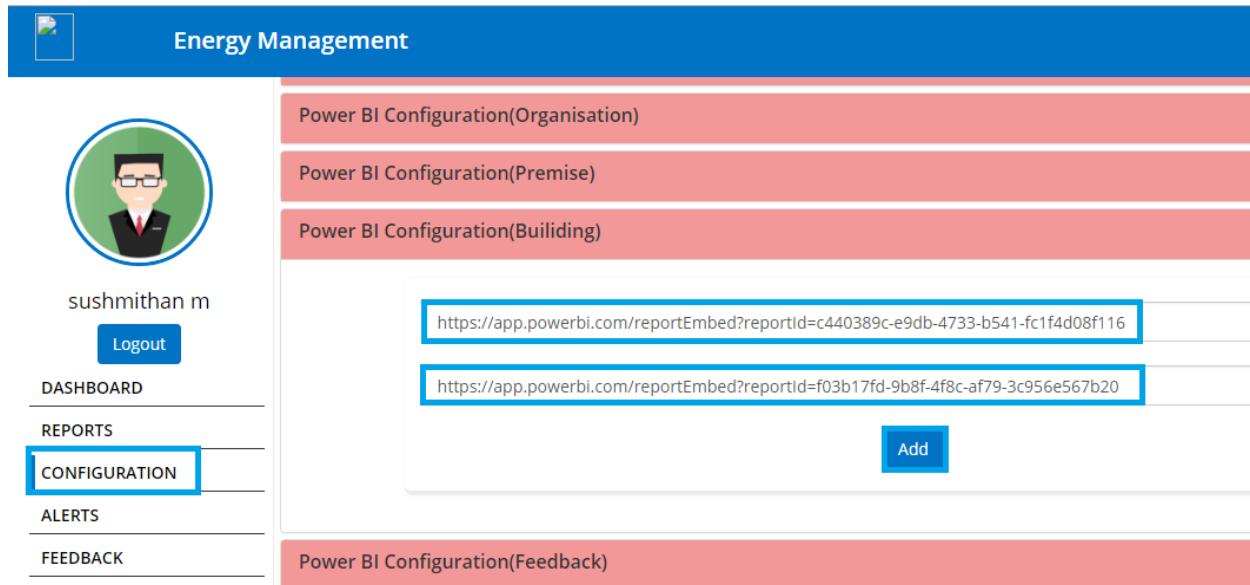
5. Once in the web app, you can view the **Dashboard** as shown below.



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**.

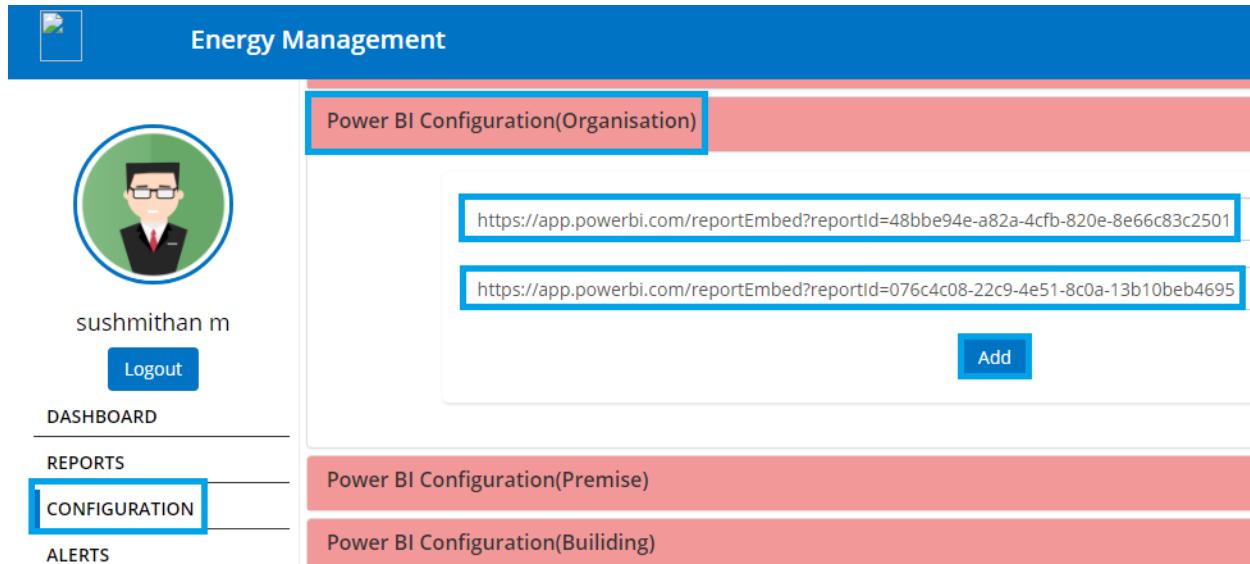


The screenshot shows the 'Energy Management' application interface. On the left, there is a sidebar with a user profile picture of a man with glasses, the name 'sushmithan m', and a 'Logout' button. Below this are navigation links: 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted with a blue border), 'ALERTS', and 'FEEDBACK'. The main content area has three tabs: 'Power BI Configuration(Organisation)', 'Power BI Configuration(Premise)', and 'Power BI Configuration(Building)'. Under 'Power BI Configuration(Organisation)', there are two URLs listed in blue boxes: <https://app.powerbi.com/reportEmbed?reportId=c440389c-e9db-4733-b541-fc1f4d08f116> and <https://app.powerbi.com/reportEmbed?reportId=f03b17fd-9b8f-4f8c-af79-3c956e567b20>. A blue 'Add' button is located at the bottom right of this section.

- 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**.

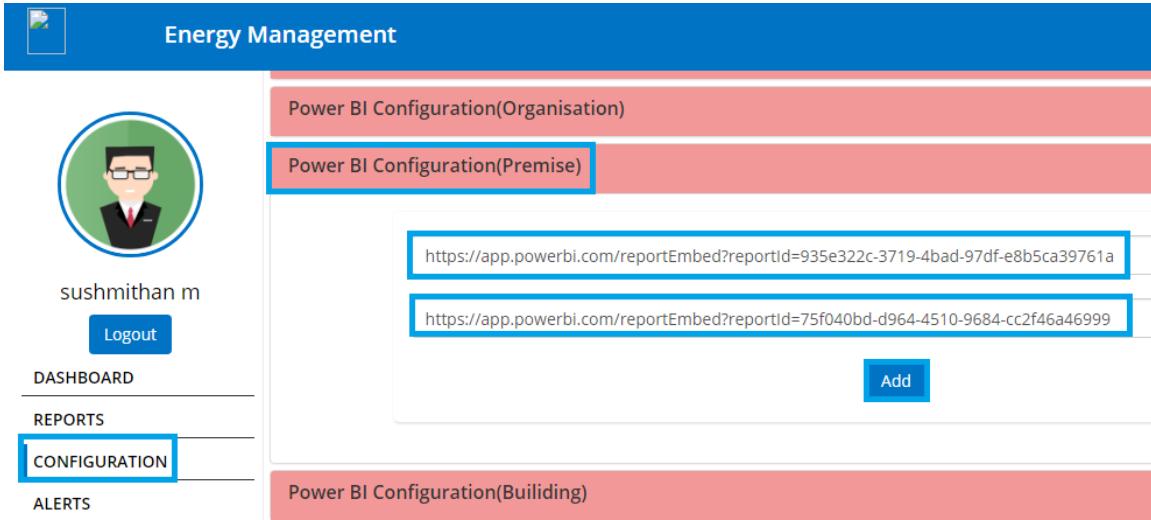


This screenshot shows the same 'Energy Management' application interface as the previous one, but with different URLs. The 'CONFIGURATION' tab is still highlighted. The 'Power BI Configuration(Organisation)' section now contains two URLs: <https://app.powerbi.com/reportEmbed?reportId=48bbe94e-a82a-4cfb-820e-8e66c83c2501> and <https://app.powerbi.com/reportEmbed?reportId=076c4c08-22c9-4e51-8c0a-13b10beb4695>. The 'Power BI Configuration(Premise)' and 'Power BI Configuration(Building)' sections are also visible below.

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

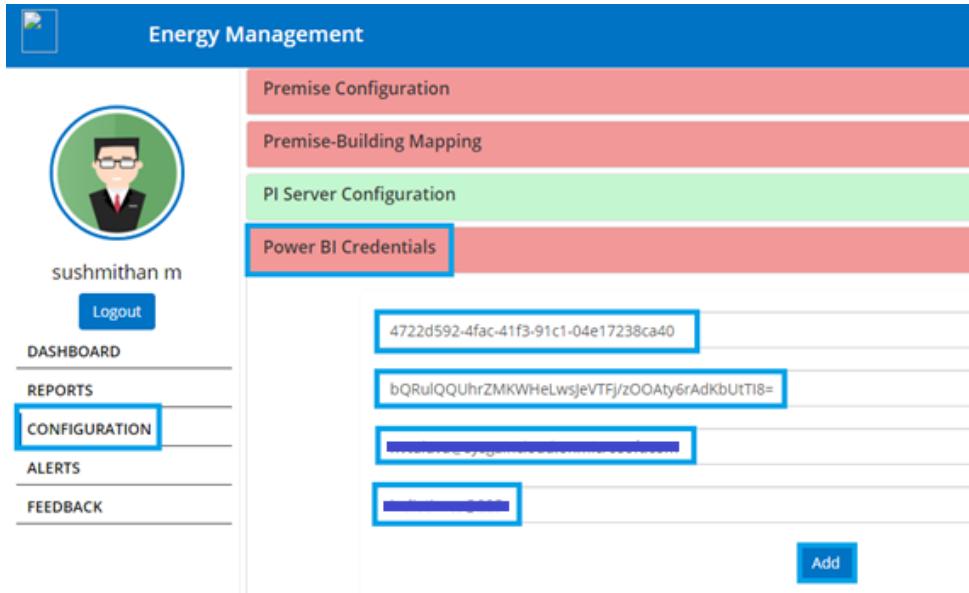
<https://app.powerbi.com/reportEmbed?reportId=<token>>

Enter them in the respective tabs (summary reports in the first column, detailed report in the second column), then click on **Add**.



The screenshot shows the 'Energy Management' application interface. On the left, there is a sidebar with a user profile picture of a man with glasses, the name 'sushmithan m', a 'Logout' button, and navigation links for 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted with a blue border), and 'ALERTS'. The main content area has a blue header bar. Below it, there are several tabs: 'Power BI Configuration(Organisation)', 'Power BI Configuration(Premise)' (which is highlighted with a blue border), 'Power BI Configuration(Building)', and 'Power BI Configuration(Builidng)'. Under the 'Power BI Configuration(Premise)' tab, there are two input fields containing URLs: 'https://app.powerbi.com/reportEmbed?reportId=935e322c-3719-4bad-97df-e8b5ca39761a' and 'https://app.powerbi.com/reportEmbed?reportId=75f040bd-d964-4510-9684-cc2f46a46999'. A blue 'Add' button is located at the bottom right of this section.

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**.



The screenshot shows the 'Energy Management' application interface. The sidebar is identical to the previous screenshot. The main content area has a blue header bar. Below it, there are four tabs: 'Premise Configuration', 'Premise-Building Mapping', 'PI Server Configuration', and 'Power BI Credentials' (which is highlighted with a blue border). Under the 'Power BI Credentials' tab, there are four input fields containing values: '4722d592-4fac-41f3-91c1-04e17238ca40', 'bQRuIQQUhrZMKWHeLwsJeVTFj/zOOAty6rAdKbUltI8=', '...', and '...'. A blue 'Add' button is located at the bottom right of this section.

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

Energy Management

ORGANIZATION SUMMARY



sushmithan m

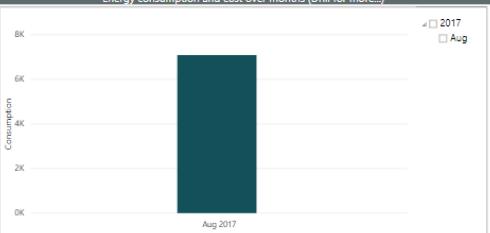
[Logout](#)

- [DASHBOARD](#)
- [REPORTS](#)
- [CONFIGURATION](#)
- [ALERTS](#)
- [FEEDBACK](#)

Organization level: Detailed Report

Electric Cost till date	Total Consumption till date (in KWh)
\$325.89	7.09K
Cost for this month	Consumption for this month (in KWh)
\$325.89	7.09K
Projected Consumption for this month (in KWh)	
OOPS !! No Data Found :(
Projected cost for this month	
OOPS !! No Data Found :(

Energy consumption and cost over months (Drill for more...)



Aug 2017

Consumption of this month VS Predicted consumption



7.09K

Prediction results will be up next month

Energy Management



sushmithan m

[Logout](#)

- [DASHBOARD](#)
- [REPORTS](#)
- [CONFIGURATION](#)
- [ALERTS](#)
- [FEEDBACK](#)

Today
Yesterday
This week
Last week
Current Month
Last Month

Consumption



Consumption Details

Filter

> □ (Blank)

Consumption: Actual VS Predicted
Microsoft Power BI

12. Machine Learning Experiment

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

40.74.240.46 - Remote Desktop Connection

- Microsoft Azure

Secure | https://portal.azure.com/#resource/subscriptions/.../resourceGroups/vivekiot1/overview

Microsoft Azure Resource groups > vivekiot1

Overview (highlighted)

Activity log

Access control (IAM)

Tags

SETTINGS

- Quickstart**
- Resource costs**
- Deployments**
- Policies**
- Properties**
- Locks**
- Automation script**

Essentials

Subscription name (change) IOT Integration Deployments 12 Succeeded

Subscription ID: 59227c217-b119-4d3b-8a13-82a1c3a16c8f

Filter by name... All types All locations Group by type

77 items

NAME	TYPE	LOCATION	...
trendServer_OsDisk_1_e2ec285b58a345ae93...	Disk	South Central US	...
MACHINE LEARNING WEB SERVICE PLAN			
workspacePlan	Machine Learning web se...	South Central US	...
MACHINE LEARNING WORKSPACE			
workspace	Machine Learning worksp...	South Central US	...
MICROSOFT.COMPUTE/RESTOREPOINTCOLLECTIONS			
AzureBackup_adServer	Microsoft.Compute/resto...	South Central US	...
AzureBackup_bastionServer	Microsoft.Compute/resto...	South Central US	...

2. Click on the **workspace**.

Resource group

Search (Ctrl+ /)

Overview (highlighted)

Activity log

Access control (IAM)

Tags

SETTINGS

- Quickstart**
- Resource costs**
- Deployments**
- Policies**
- Properties**
- Locks**
- Automation script**

MONITORING

Essentials

Subscription name (change) IOT Integration Deployments 12 Succeeded

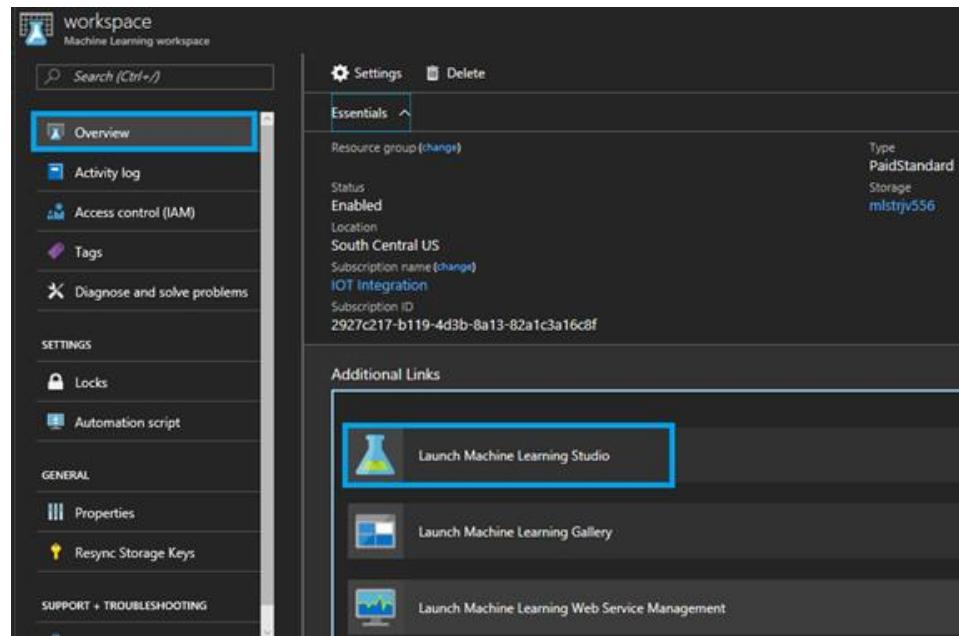
Subscription ID: 2927c217-b119-4d3b-8a13-82a1c3a16c8f

Filter by name... All types All locations Group by type

69 items

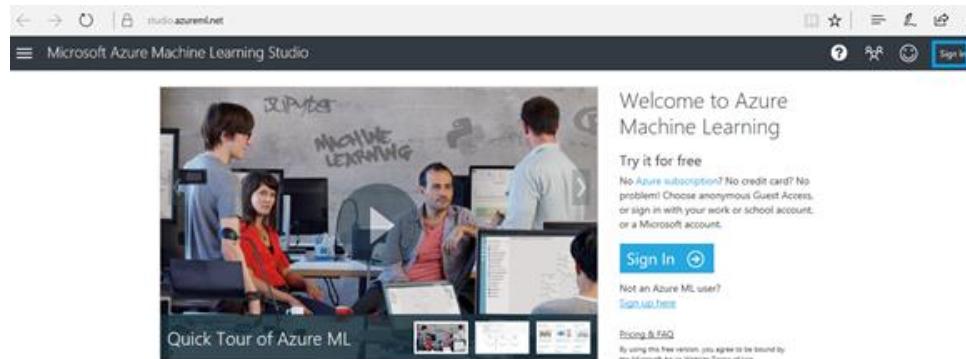
NAME	TYPE	LOCATION	...
splunkserver_disk2_b77ad5351b934e699fea...	Disk	South Central US	...
splunkserver_OsDisk_1_da289fface4425a8e...	Disk	South Central US	...
trendServer_OsDisk_1_e2ec285b58a345ae93...	Disk	South Central US	...
MACHINE LEARNING WEB SERVICE PLAN			
workspacePlan	Machine Learning web se...	South Central US	...
MACHINE LEARNING WORKSPACE			
workspace	Machine Learning worksp...	South Central US	...
NETWORK INTERFACE			
adNic	Network interface	South Central US	...

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



The screenshot shows the 'Overview' section of a 'Machine Learning workspace'. The left sidebar includes links for 'Search (Ctrl+)', 'Overview' (which is selected and highlighted with a blue border), 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Locks', 'Automation script', 'Properties', and 'Resync Storage Keys'. The main content area displays 'Essentials' settings: Resource group (changed), Status (Enabled), Location (South Central US), Subscription name (change), IOT Integration, and Subscription ID (2927c217-b119-4d3b-8a13-82a1c3a16c8f). Below this is an 'Additional Links' section with three items: 'Launch Machine Learning Studio' (highlighted with a blue border), 'Launch Machine Learning Gallery', and 'Launch Machine Learning Web Service Management'.

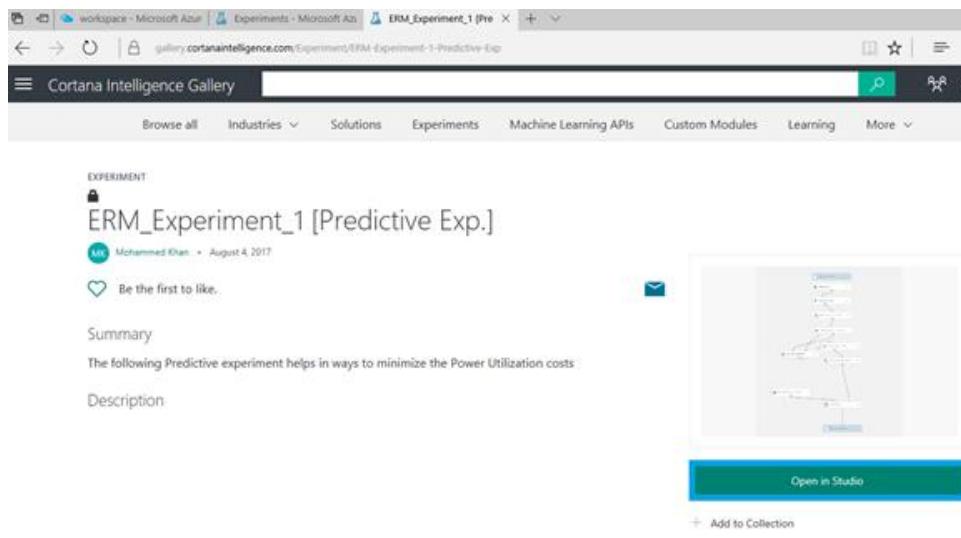
4. Sign in to the Microsoft Azure Machine Learning Studio.



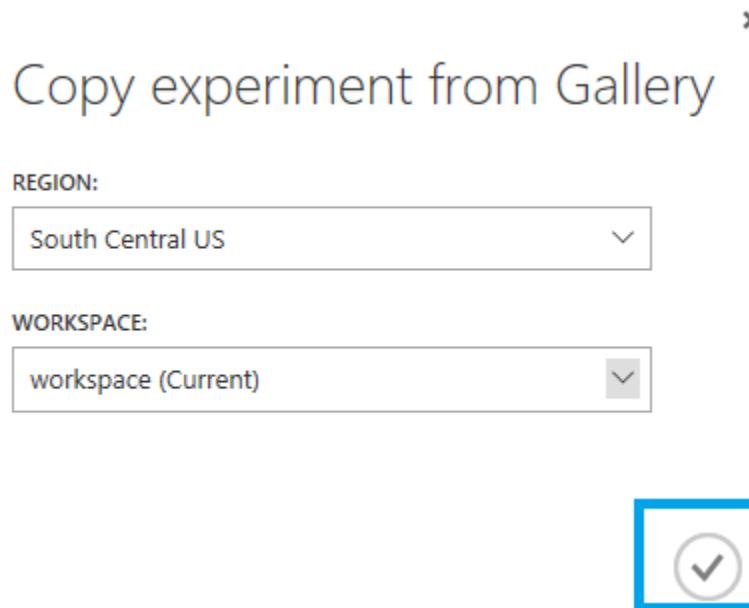
The screenshot shows the Microsoft Azure Machine Learning Studio landing page. It features a banner with four people working on computers in front of a 'DATA SCIENCE' and 'MACHINE LEARNING' wall. Below the banner is a 'Quick Tour of Azure ML' button. To the right, there's a 'Welcome to Azure Machine Learning' message, a 'Try it for free' section with guest access information, a 'Sign In' button, and a note for non-Azure ML users. At the bottom, there's a 'Pricing & FAQ' link and a terms of use disclaimer.

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

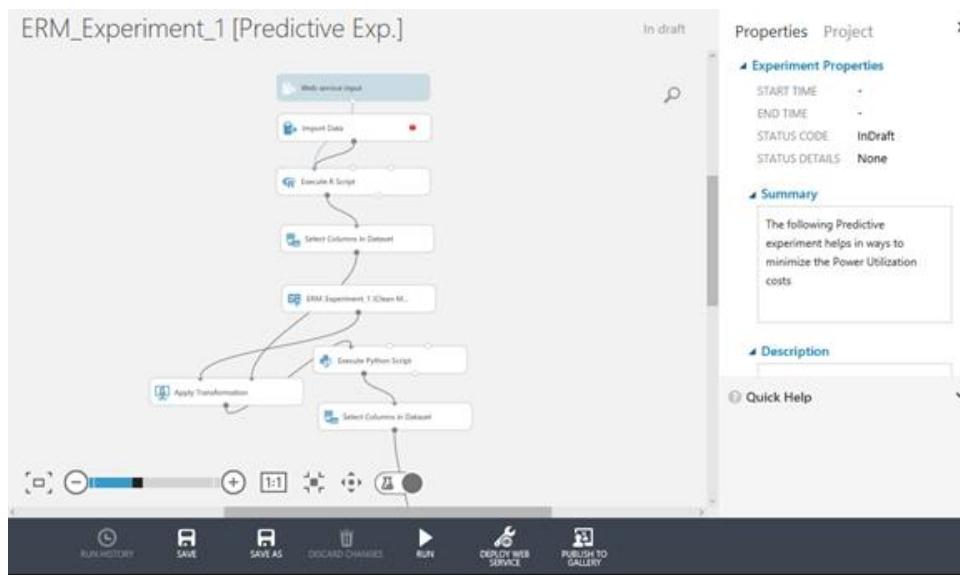
Path : <https://gallery.cortaintelligence.com/Experiment/ERM-Experiment-1-Predictive-Exp>



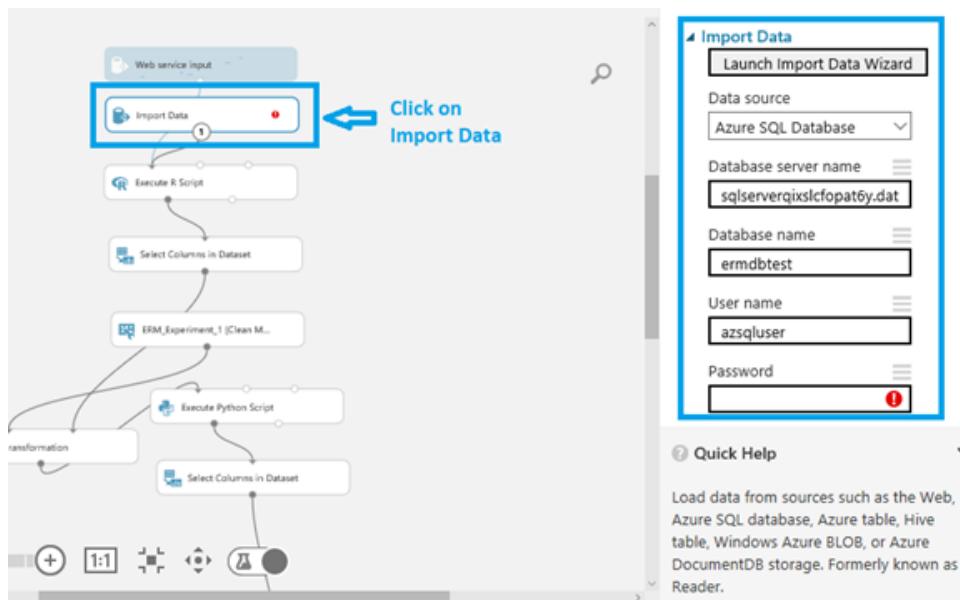
6. The below screen will appear in the new tab, click on the **check mark**.



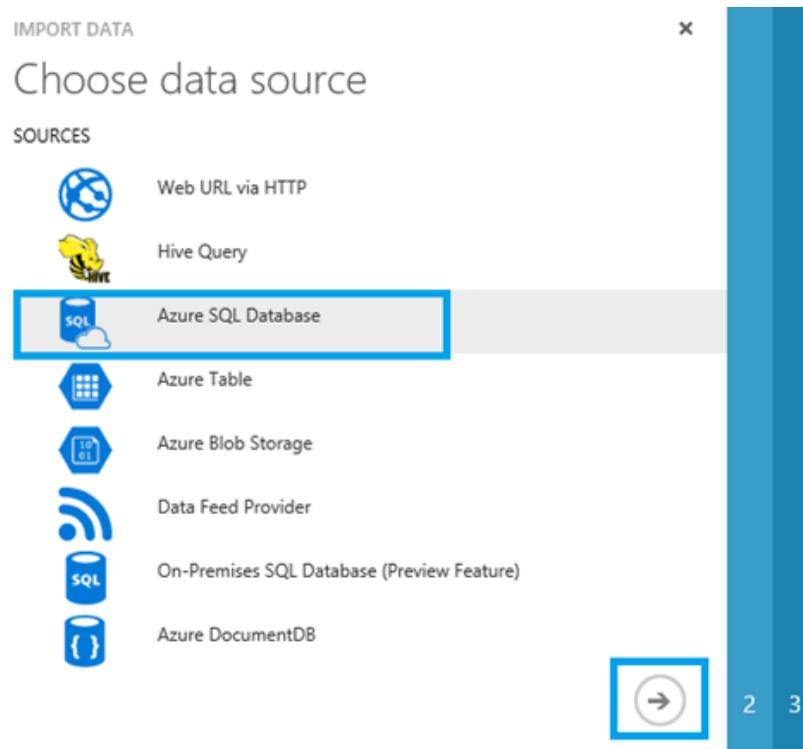
7. The experiment will be downloaded to the workspace.



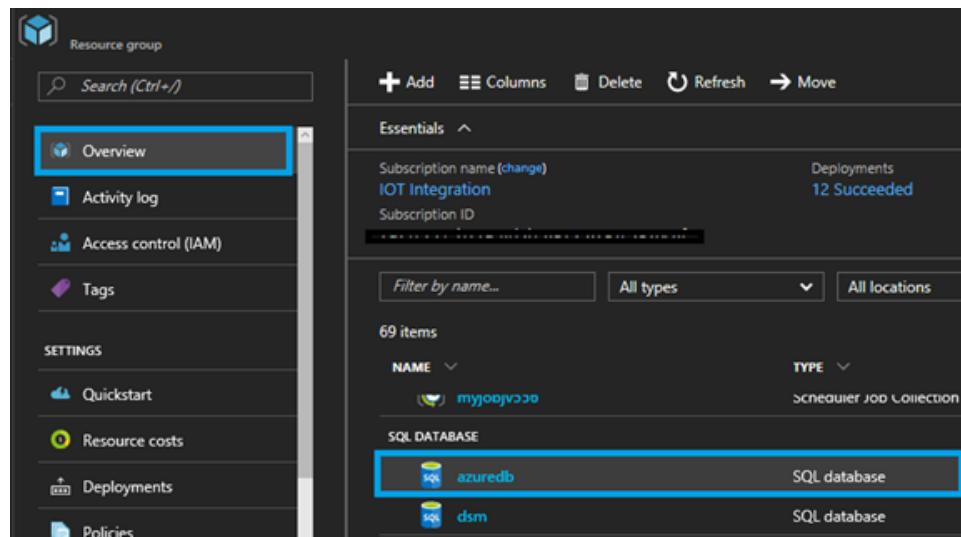
8. Once the experiment is pulled into the workspace, click on **Import Data**. Then click on **Launch Import Data Wizard** from right side menu.



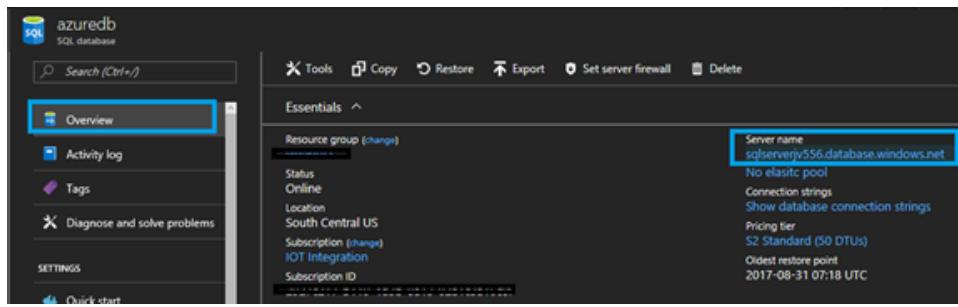
9. Select **Azure SQL Database** and click on Next icon “->”.



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



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



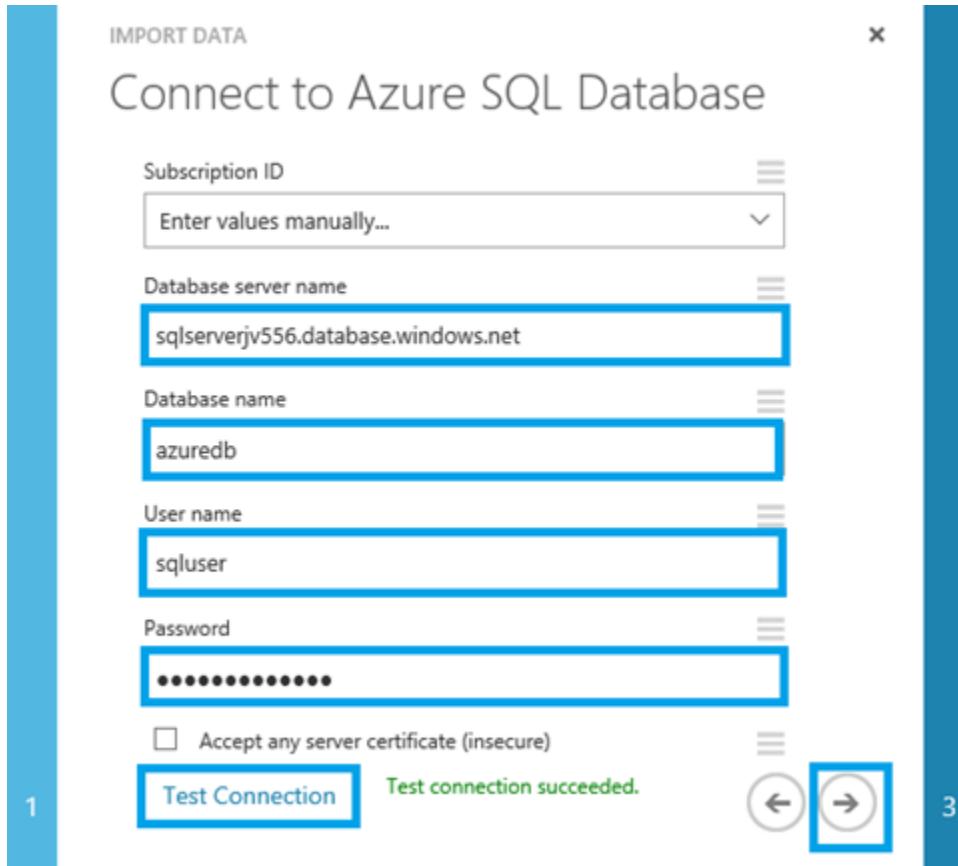
The screenshot shows the Azure portal interface for a SQL database named 'azuredb'. The left sidebar has 'Overview' selected. The main pane shows the 'Essentials' section with various details. The 'Server name' field is highlighted with a blue box.

Resource group (change)	Server name
Status Online Location South Central US Subscription (Change) IOT Integration Subscription ID	sqlserverjv556.database.windows.net No elastic pool Connection strings Show database connection strings Pricing tier S2 Standard (50 DTUs) Oldest restore point 2017-08-31 07:18 UTC

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

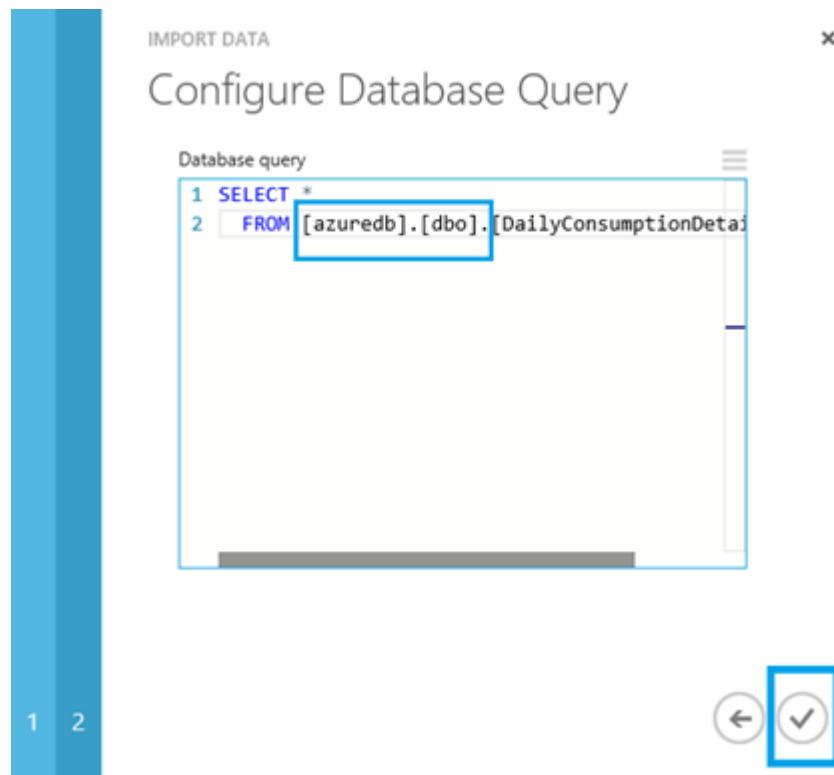
Enter the **Database name**, **User name**, and **Password**, then click on **Test Connection**.

After the test connection succeeds, click on Next icon.

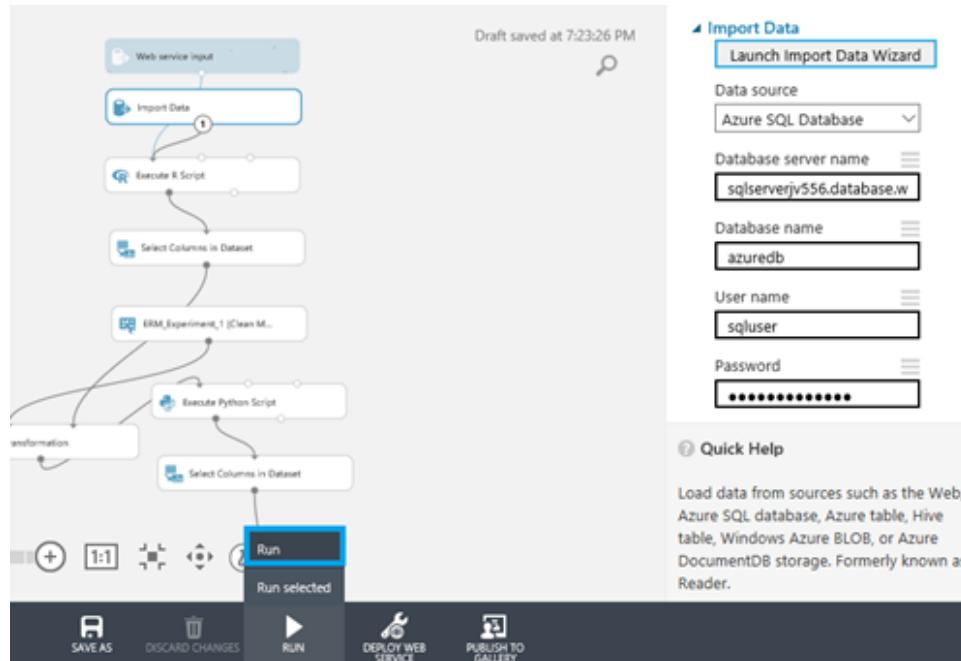


The screenshot shows the 'Connect to Azure SQL Database' dialog box. It includes fields for Subscription ID, Database server name (set to 'sqlserverjv556.database.windows.net'), Database name ('azuredb'), User name ('sqouser'), Password ('*****'), and an 'Accept any server certificate (insecure)' checkbox. Below the fields are two buttons: 'Test Connection' (highlighted with a blue box) and 'Test connection succeeded.' A navigation bar at the bottom shows steps 1, 2, and 3.

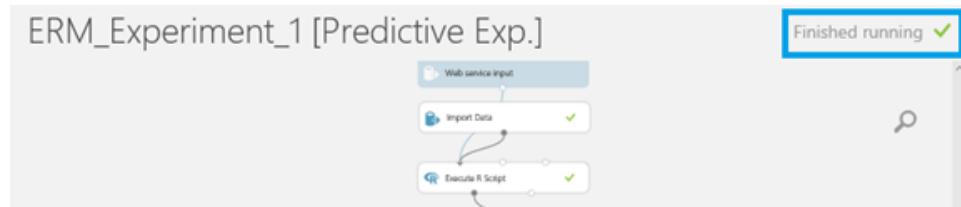
13. Replace the Database name with **azuredb** and click on the **check mark**.



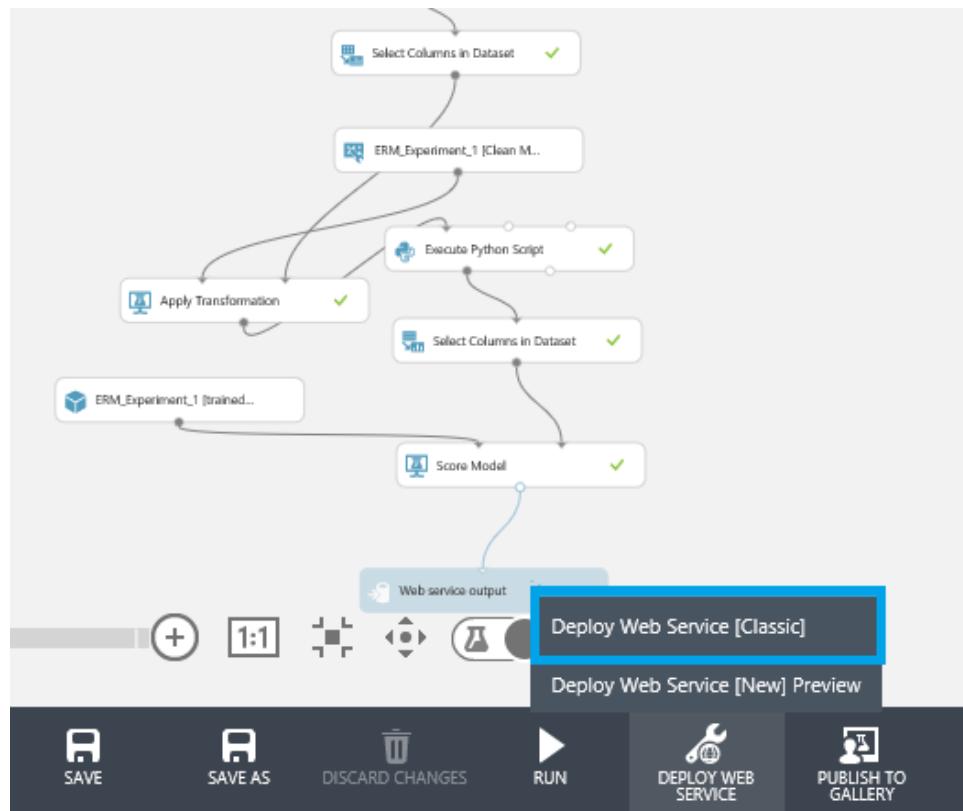
14. Once done, run the experiment by right clicking on **Run** from bottom of the below screen, and select **Run** from the dropdown menu.



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**.

erm_experiment_1 [predictive exp.]

DASHBOARD CONFIGURATION

General [New Web Services Experience](#) preview

Published experiment

[View snapshot](#) [View latest](#)

Description

No description provided for this web service.

API key

```
+n92PDuzx70O/tputyGUKRfls0Ul0AaCgbqmhZ03PjCxoIWwww4J0Q7+tDaUEME5B1DFwxzgVbB+aOP0Lh5Ssag==
```

Default Endpoint

[API HELP PAGE](#)

TEST

APPS

[REQUEST/RESPONSE](#)

Test preview

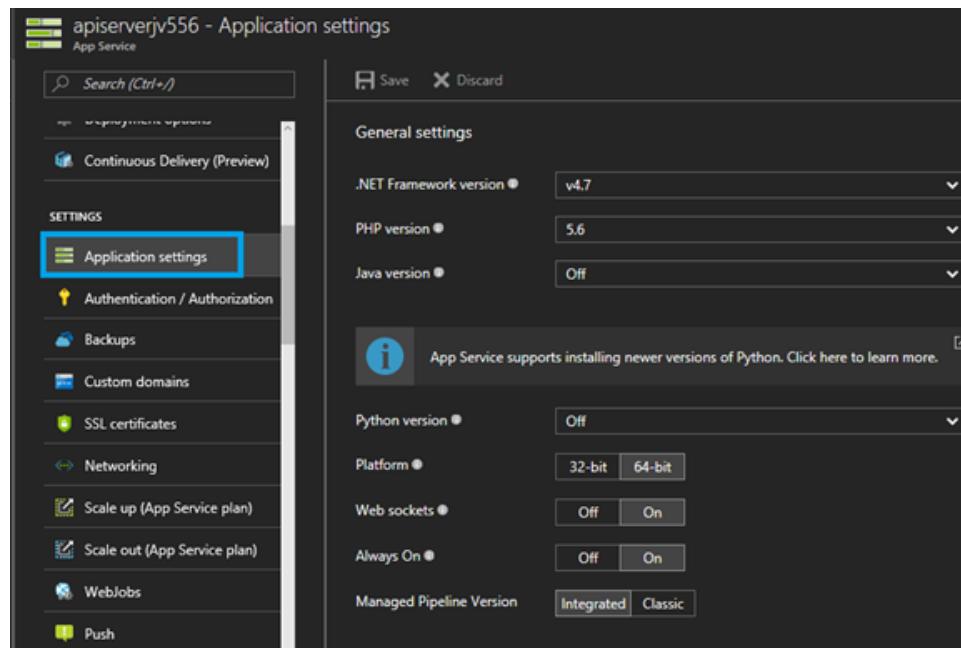
 Excel 2013 or later

[BATCH EXECUTION](#)

Test preview

 Excel 2013 or later

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**.

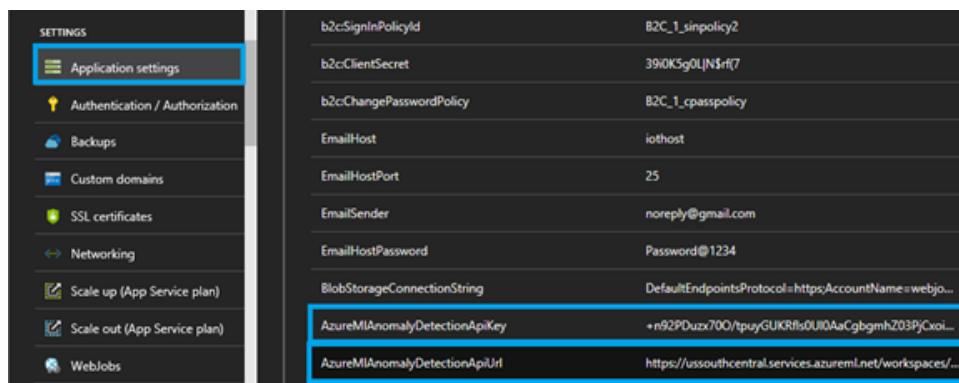


The screenshot shows the 'Application settings' blade for an App Service named 'apiserverjv556'. The left sidebar lists various settings like Continuous Delivery, Application settings (which is selected and highlighted with a blue box), Authentication / Authorization, Backups, Custom domains, SSL certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), WebJobs, and Push. The main area is titled 'General settings' and includes dropdowns for .NET Framework version (v4.7), PHP version (5.6), Java version (Off), Python version (Off), Platform (32-bit/64-bit), Web sockets (Off/On), Always On (Off/On), and Managed Pipeline Version (Integrated/Classic). A note at the bottom states: 'App Service supports installing newer versions of Python. Click here to learn more.'

21. Add

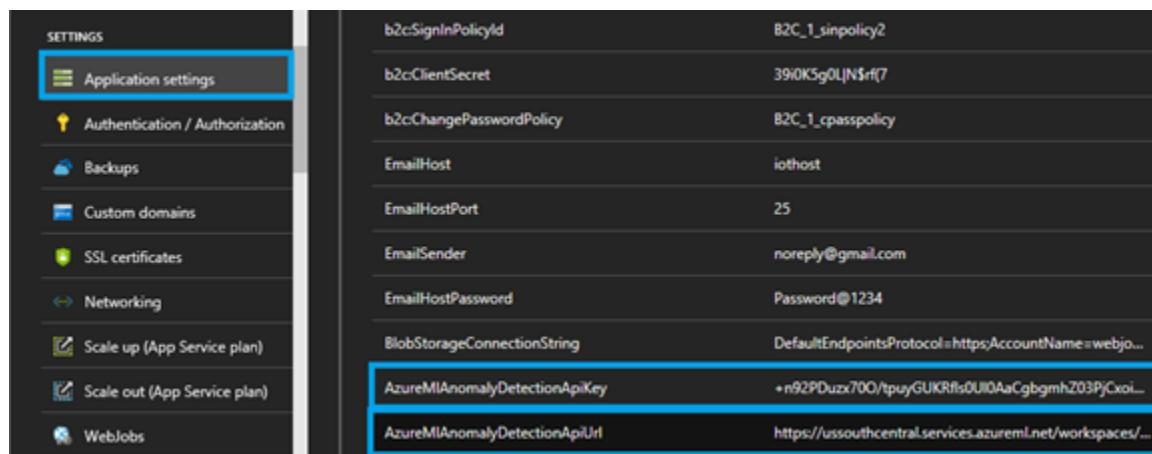
AzureMIAnomalyDetectionApiKey with apikey value from **step 17**.

AzureMIAnomalyDetectionApiUrl with Post URL from step 18.



b2cSignInPolicyId	B2C_1_sinpolicy2
b2cClientSecret	39iOK5g0LjN\$rlf7
b2cChangePasswordPolicy	B2C_1_cpasspolicy
EmailHost	iohost
EmailHostPort	25
EmailSender	noreply@gmail.com
EmailHostPassword	Password@1234
BlobStorageConnectionString	DefaultEndpointsProtocol=https;AccountName=webjo...
AzureMIAnomalyDetectionApiKey	+n92PDuzx700/tpuyGUKRfls0UI0AaCgbgmhZ03PjCxoi...
AzureMIAnomalyDetectionApiUrl	https://ussouthcentral.services.azureml.net/workspaces/...

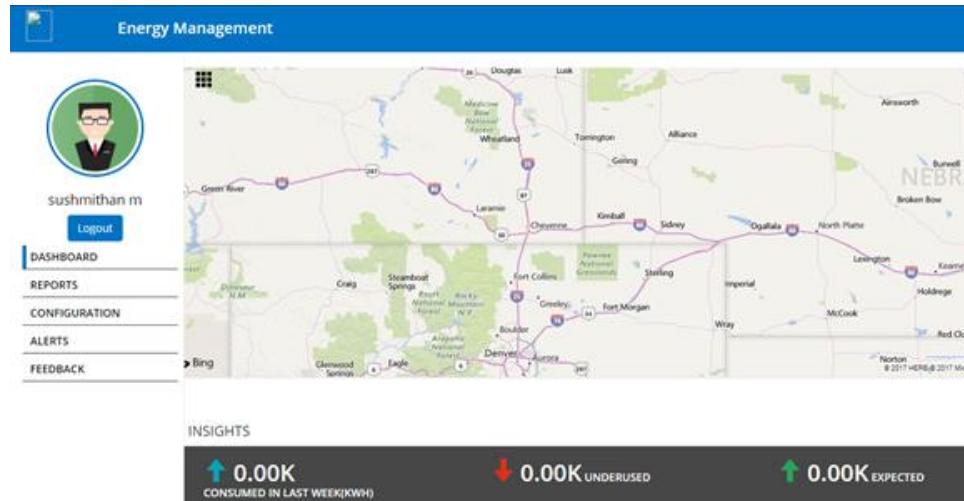
22. Restart the **apiserver**.



b2cSignInPolicyId	B2C_1_sinpolicy2
b2cClientSecret	39iOK5g0LjN\$rlf7
b2cChangePasswordPolicy	B2C_1_cpasspolicy
EmailHost	iohost
EmailHostPort	25
EmailSender	noreply@gmail.com
EmailHostPassword	Password@1234
BlobStorageConnectionString	DefaultEndpointsProtocol=https;AccountName=webjo...
AzureMIAnomalyDetectionApiKey	+n92PDuzx700/tpuyGUKRfls0UI0AaCgbgmhZ03PjCxoi...
AzureMIAnomalyDetectionApiUrl	https://ussouthcentral.services.azureml.net/workspaces/...

23. Login to the web application.



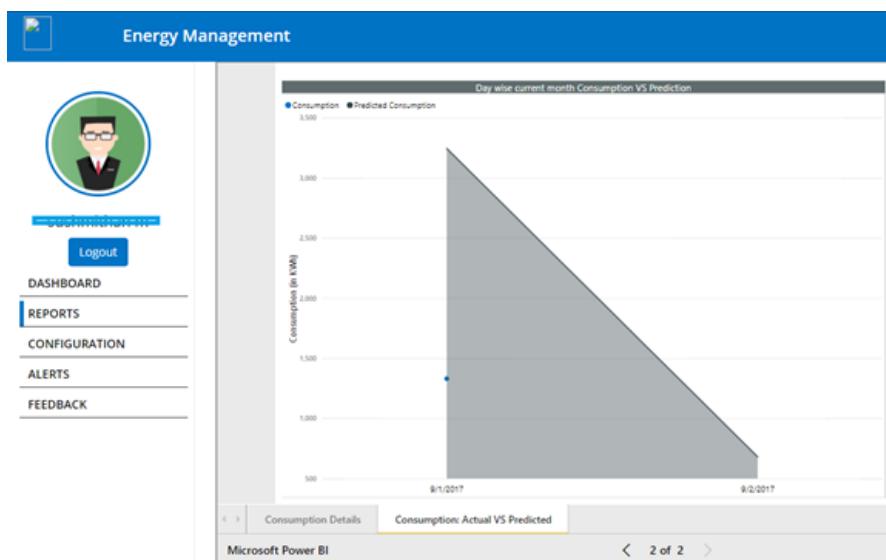


24. Navigate to **Azure ML Configuration** and add the **API Key** and **POST URL**.

Click on **Add**.

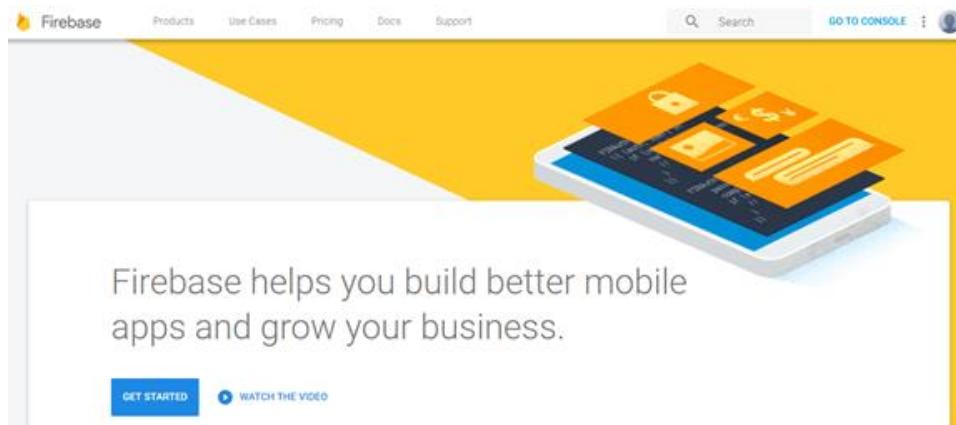


25. Click on **REPORTS** and click on **Consumption: Actual VS Predicted** of the bottom of the screen to view the Actual Vs Predicted graph.

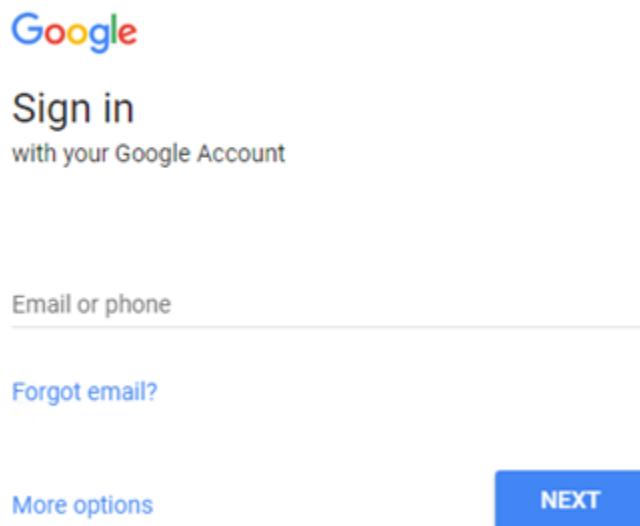


13. Firebase Configuration

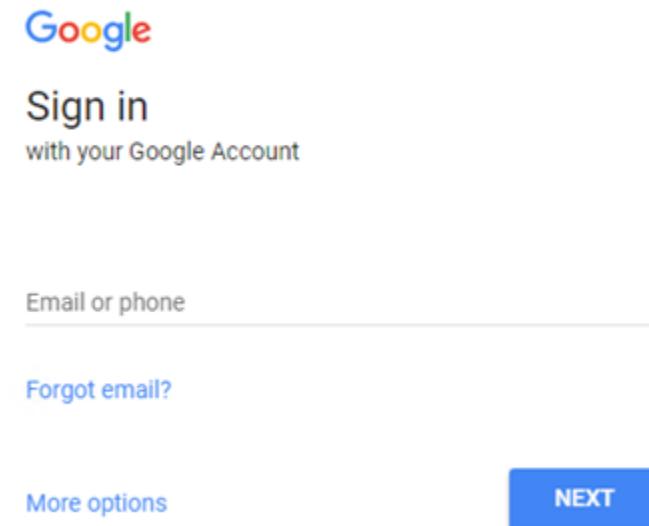
1. Go to the <https://firebase.google.com> URL and click on **GO TO CONSOLE**.



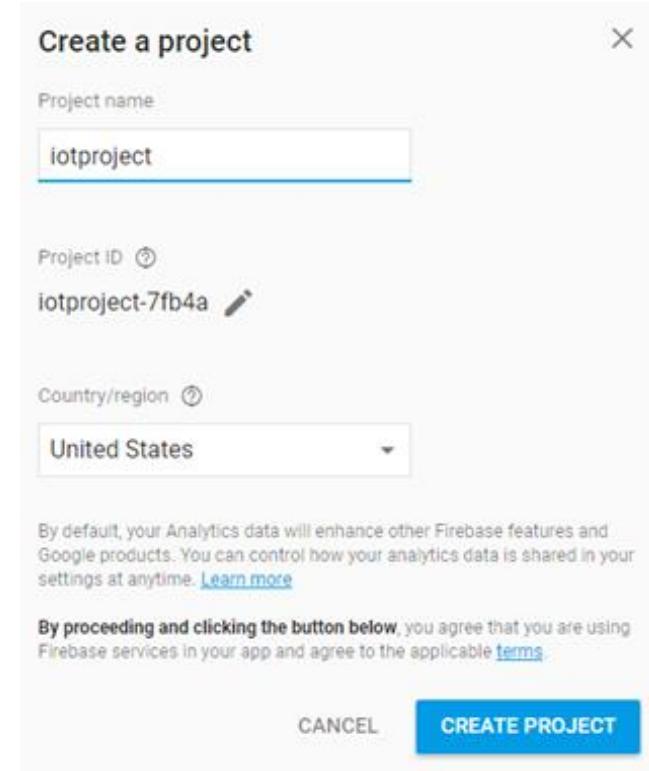
2. Sign in with your Gmail credentials.



3. Click on **Add Project**.

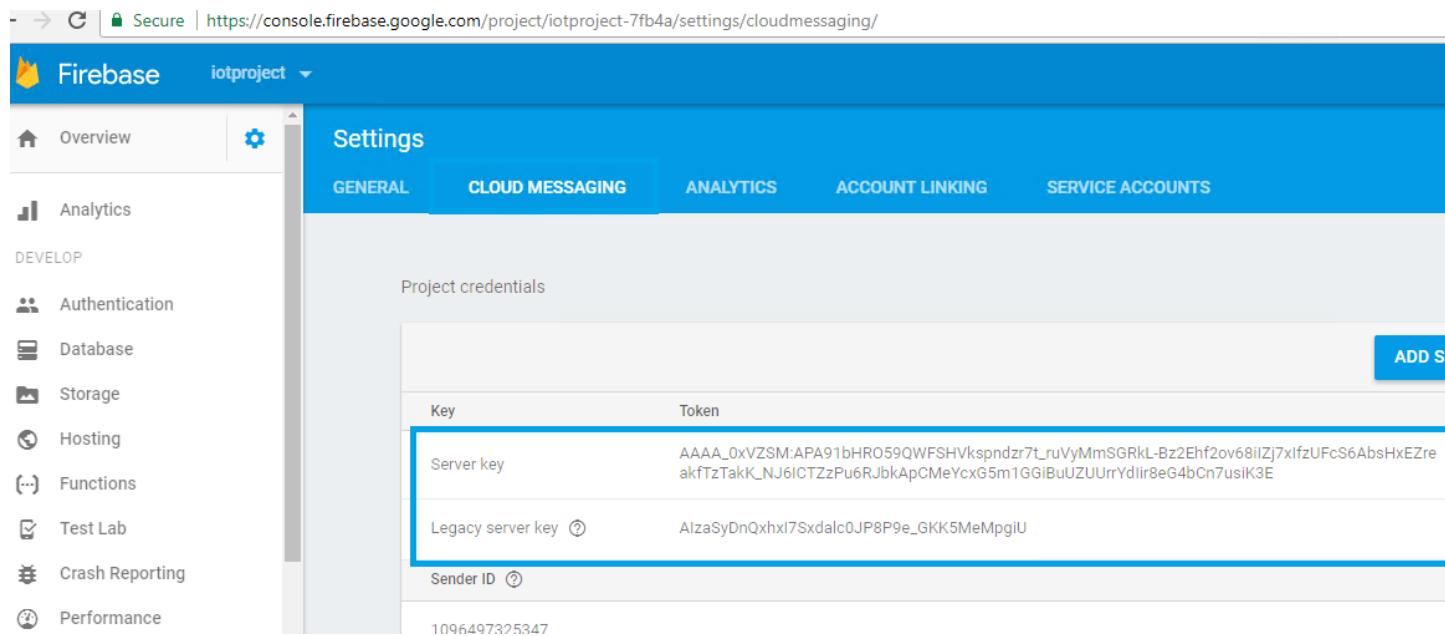


4. Give a **Project name** and click on **CREATE PROJECT**.

A screenshot of the "Create a project" dialog box. The title bar says "Create a project" and has a close button "X".

- Project name:** A text input field containing "iotproject".
- Project ID:** A text input field containing "iotproject-7fb4a" with a pencil icon for editing.
- Country/region:** A dropdown menu set to "United States".
- By default, your Analytics data will enhance other Firebase features and Google products. You can control how your analytics data is shared in your settings at anytime. [Learn more](#)
- By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable [terms](#).
- CANCEL** and **CREATE PROJECT** buttons at the bottom.

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

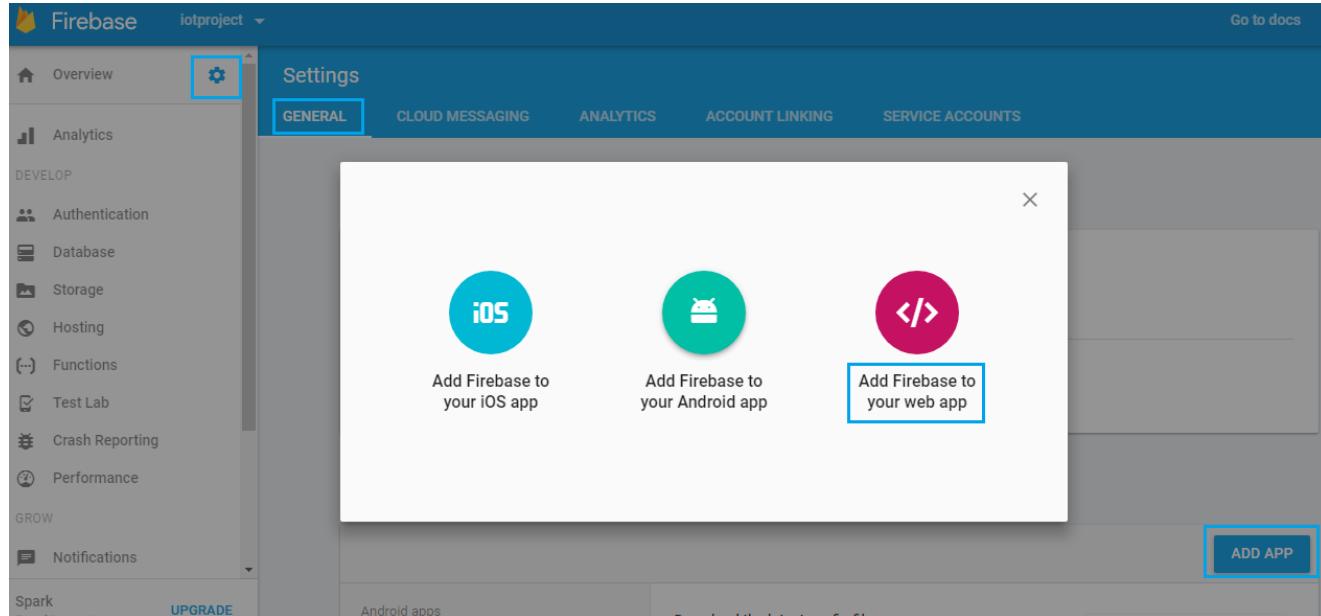


The screenshot shows the Firebase console for a project named "iotproject". The left sidebar includes links for Overview, Analytics, Database, Storage, Hosting, Functions, Test Lab, Crash Reporting, and Performance. The main area is titled "Settings" with tabs for GENERAL, CLOUD MESSAGING (which is selected), ANALYTICS, ACCOUNT LINKING, and SERVICE ACCOUNTS. Under "Project credentials", there is a table with two rows:

Key	Token
Server key	AAAA_0xVZSM:APA91bHR059QWFShVksPndzr7t_ruVyMmSGRkL-Bz2Ehf2ov68iJz7xifUFcS6AbsHxEZreakfTzTakK_NJ6ICTZzPu6RJbkApCMeYcxG5m1GGIBuUZUrrYdlr8eG4bCn7uslK3E
Legacy server key	AlzaSyDnQxhl7Sxdalc0JP8P9e_GKK5MeMpgiU

Below the table, the "Sender ID" is listed as 1096497325347.

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.



The screenshot shows the Firebase console with the "GENERAL" tab selected in the top navigation bar. On the right, a modal window is open with three options: "iOS", "Android", and "Web". The "Web" option, which has a pink icon with a white double slash symbol, is highlighted with a blue border. A large blue button labeled "ADD APP" is located at the bottom right of the modal.

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

Add Firebase to your web app X

Copy and paste the snippet below at the bottom of your HTML, before other `script` tags.

```
<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
  // Initialize Firebase
  var config = {
    apiKey: "AlzaSyAbTdFA76Xo5THJRqIdRWLfDn63uYGhIo8",
    authDomain: "iotproject-7fb4a.firebaseio.com",
    databaseURL: "https://iotproject-7fb4a.firebaseio.com",
    projectId: "iotproject-7fb4a",
    storageBucket: "iotproject-7fb4a.appspot.com",
    messagingSenderId: "1096497325347"
  };
  firebase.initializeApp(config);
</script>
```

[COPY](#)

Check these resources to learn more about Firebase for web apps:

[Get Started with Firebase for Web Apps](#) ↗
[Firebase Web SDK API Reference](#) ↗
[Firebase Web Samples](#) ↗

```
<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
  // Initialize Firebase
  var config = {
    apiKey: "AlzaSyAbTdFA76Xo5THJRqIdRWLfDn63uYGhIo8",
    authDomain: "iotproject-7fb4a.firebaseio.com",
    databaseURL: "https://iotproject-7fb4a.firebaseio.com",
    projectId: "iotproject-7fb4a",
    storageBucket: "iotproject-7fb4a.appspot.com",
    messagingSenderId: "1096497325347"
  };
  firebase.initializeApp(config);
</script>
```

9. Open postman

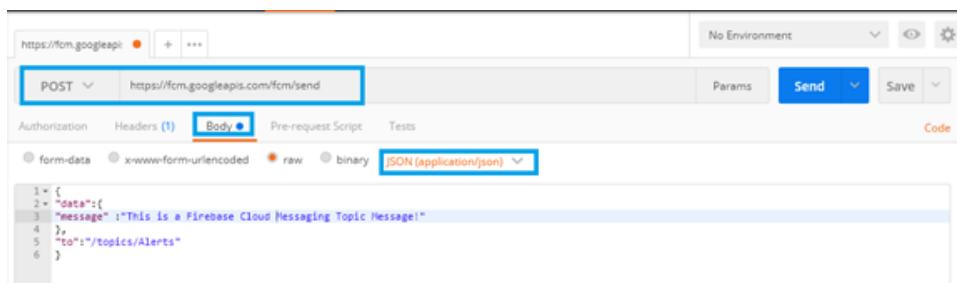
- Change the Params to **POST** and paste the below URL

<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**



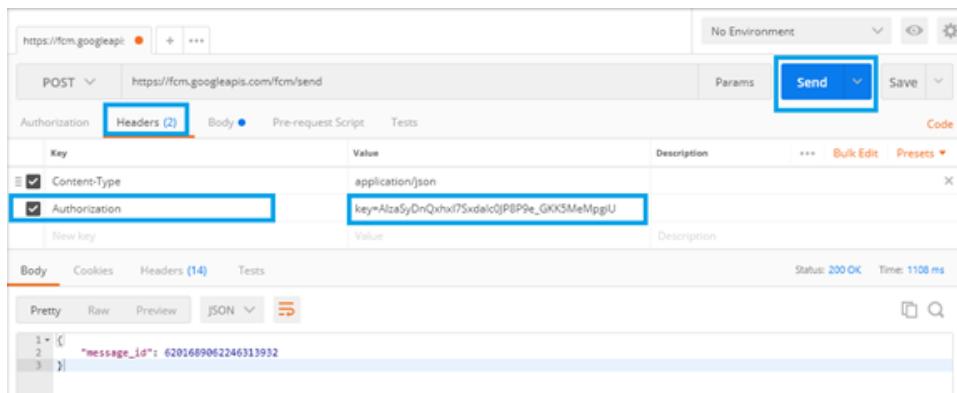
The screenshot shows the Postman interface with a POST request to <https://fcm.googleapis.com/fcm/send>. The 'Body' tab is selected, and the content type is set to 'JSON (application/json)'. The JSON payload is as follows:

```

1 {
2   "data":{
3     "message" :"This is a Firebase Cloud Messaging Topic Message!"
4   },
5   "to":"/topics/Alerts"
6 }

```

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**.



The screenshot shows the Postman interface with the 'Headers' tab selected. A new header 'Authorization' is added with the value 'key=Alza5yDrQxhxI7Sxdalc0jPBP9e_GKKSMeMpgiU'. The 'Send' button is highlighted.

Key	Value	Description
Content-Type	application/json	
Authorization	key=Alza5yDrQxhxI7Sxdalc0jPBP9e_GKKSMeMpgiU	

The response status is 200 OK with a time of 1108 ms. The JSON response body is:

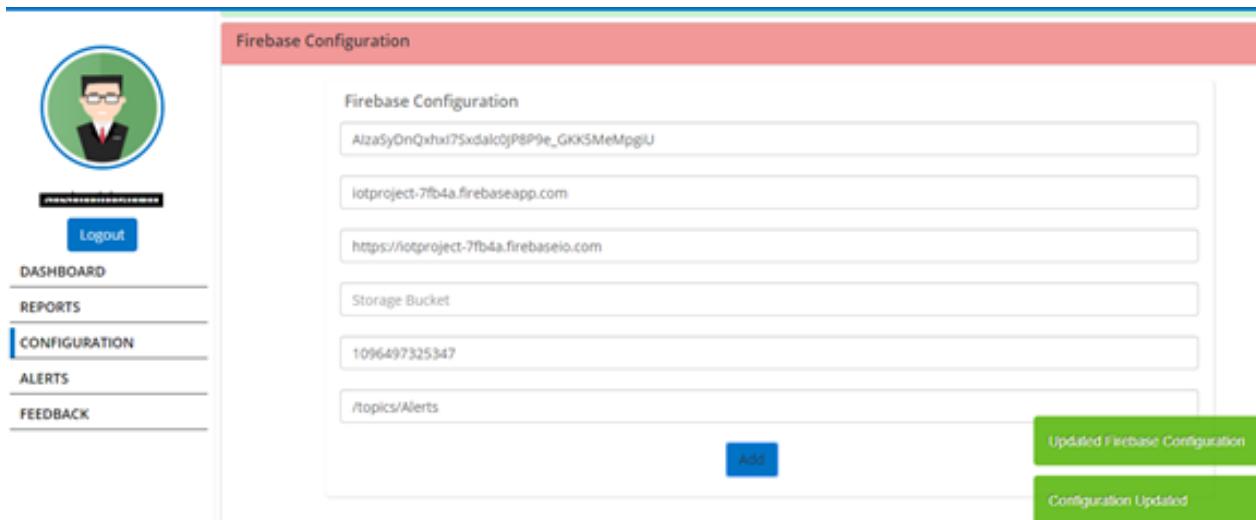
```

1 {
2   "message_id": "6201689062246313932"
3 }

```

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**



The screenshot shows the 'Firebase Configuration' page. On the left is a sidebar with a user profile picture, a 'Logout' button, and a navigation menu with links: DASHBOARD, REPORTS, CONFIGURATION (which is highlighted), ALERTS, and FEEDBACK. The main area has a red header bar labeled 'Firebase Configuration'. Below it are five input fields: 'Firebase Configuration' containing 'Alza5yOnQxhJ75xdalc0jP8P9e_GKK5MeMpgIU', 'Project ID' containing 'iotproject-7fb4a.firebaseio.com', 'URL' containing 'https://iotproject-7fb4a.firebaseio.com', 'Storage Bucket' containing '1096497325347', and 'Messaging Reviewer ID' containing '/topics/Alerts'. A blue 'Add' button is located at the bottom of the configuration section. To the right of the configuration section is a green button labeled 'Configuration Updated'.

14. Restore Virtual Machines

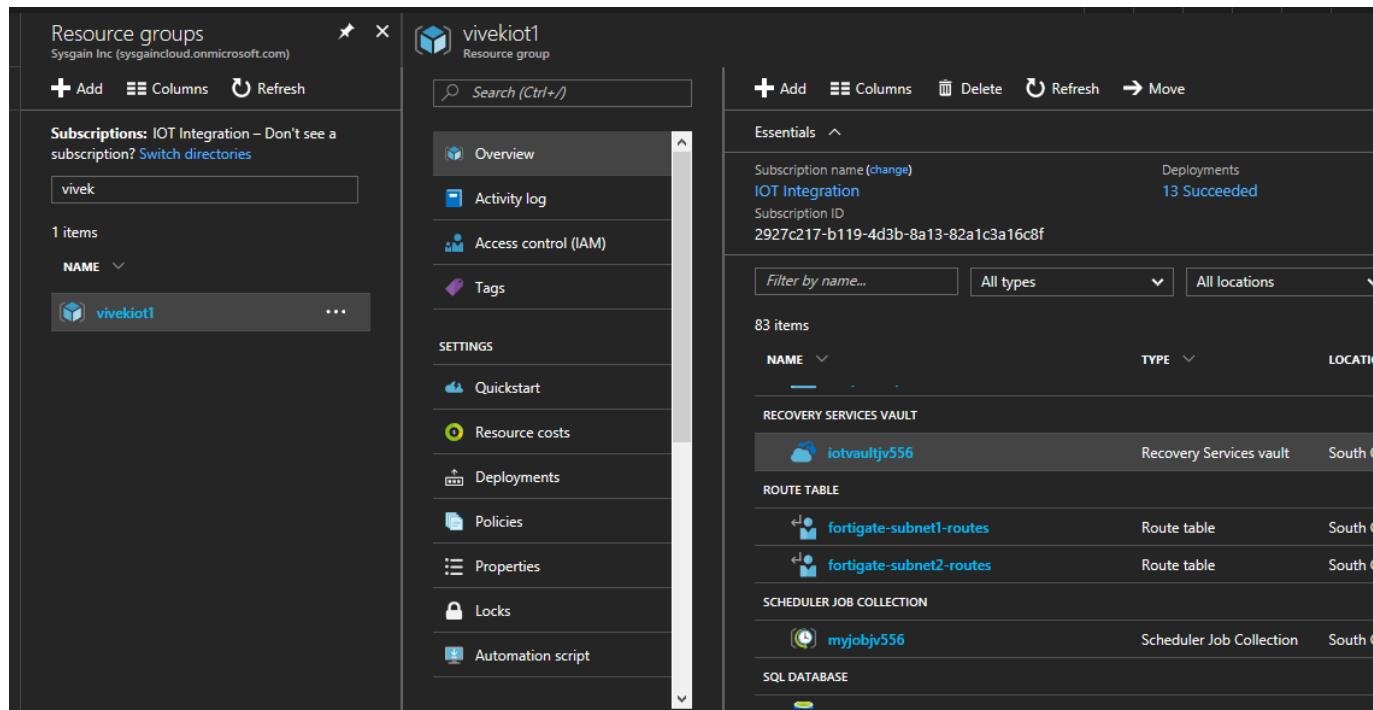
Protect your data by taking snapshots of your data at defined intervals. These snapshots are known as recovery points, and they are stored in recovery services vaults. If or when it is necessary to repair or rebuild a VM, you can restore the VM from any of the saved recovery points. When you restore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



The screenshot shows the Azure portal interface. On the left, the 'Resource groups' blade is open, displaying a single item named 'vivek'. In the center, the 'vivekiot1' resource group dashboard is shown. The dashboard includes a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, and Automation script. Below the navigation menu, there are sections for Essentials, Recovery Services Vault, Route Table, Scheduler Job Collection, and SQL Database. The 'Essentials' section shows a subscription name (IOT Integration), Subscription ID (2927c217-b119-4d3b-8a13-82a1c3a16c8f), and 13 succeeded deployments. The 'Recovery Services Vault' section lists 'iotvaultjv556' as a Recovery Services vault located in South Central US. The 'Route Table' section lists two route tables: 'fortigate-subnet1-routes' and 'fortigate-subnet2-routes'. The 'Scheduler Job Collection' section lists 'myjobjv556' as a Scheduler Job Collection located in South Central US. The 'SQL Database' section is currently empty.

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

iotvaultjv556
Recovery Services vault

Search (Ctrl+ /)

Backup **Replicate** **Delete**

We are listening. Tell us about your experience with Azure Backup and / or Azure Site Recovery and help us improve our product. Take the survey now!

Essentials

Resource group (change) vivekiot1	Backup items 8
Status Active	Backup management servers 0
Location South Central US	Replicated items 0
Subscription name (change) IOT Integration	
Subscription ID 2927c217-b119-4d3b-8a13-82a1c3a16c8f	

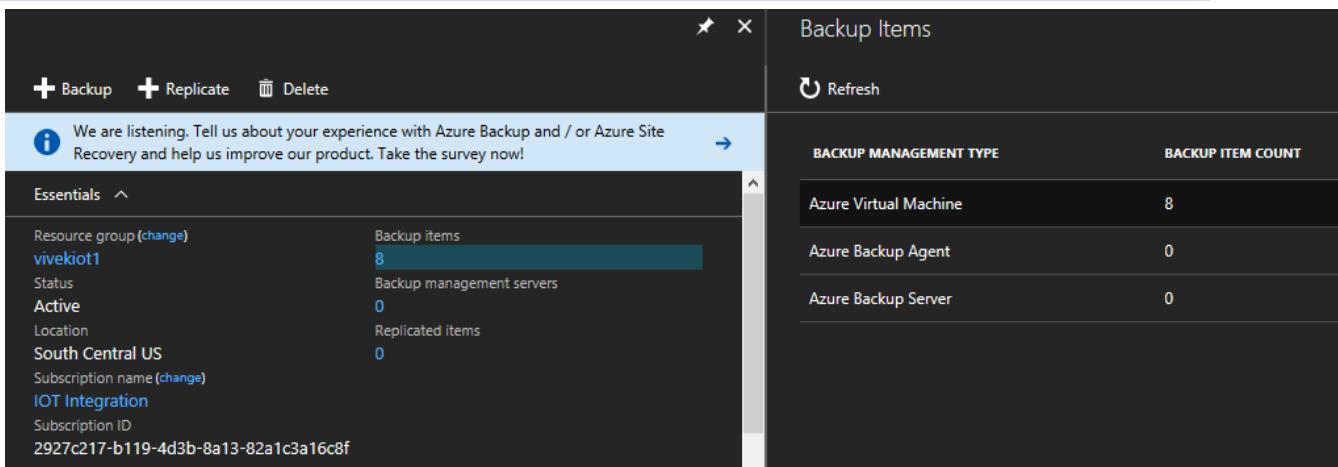
Monitoring

Backup Alerts (last 24...)		Backup Pre-Check Status (Azure VMs)	
Critical	0	CRITICAL	0
Warning	0	WARNING	1



- 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.

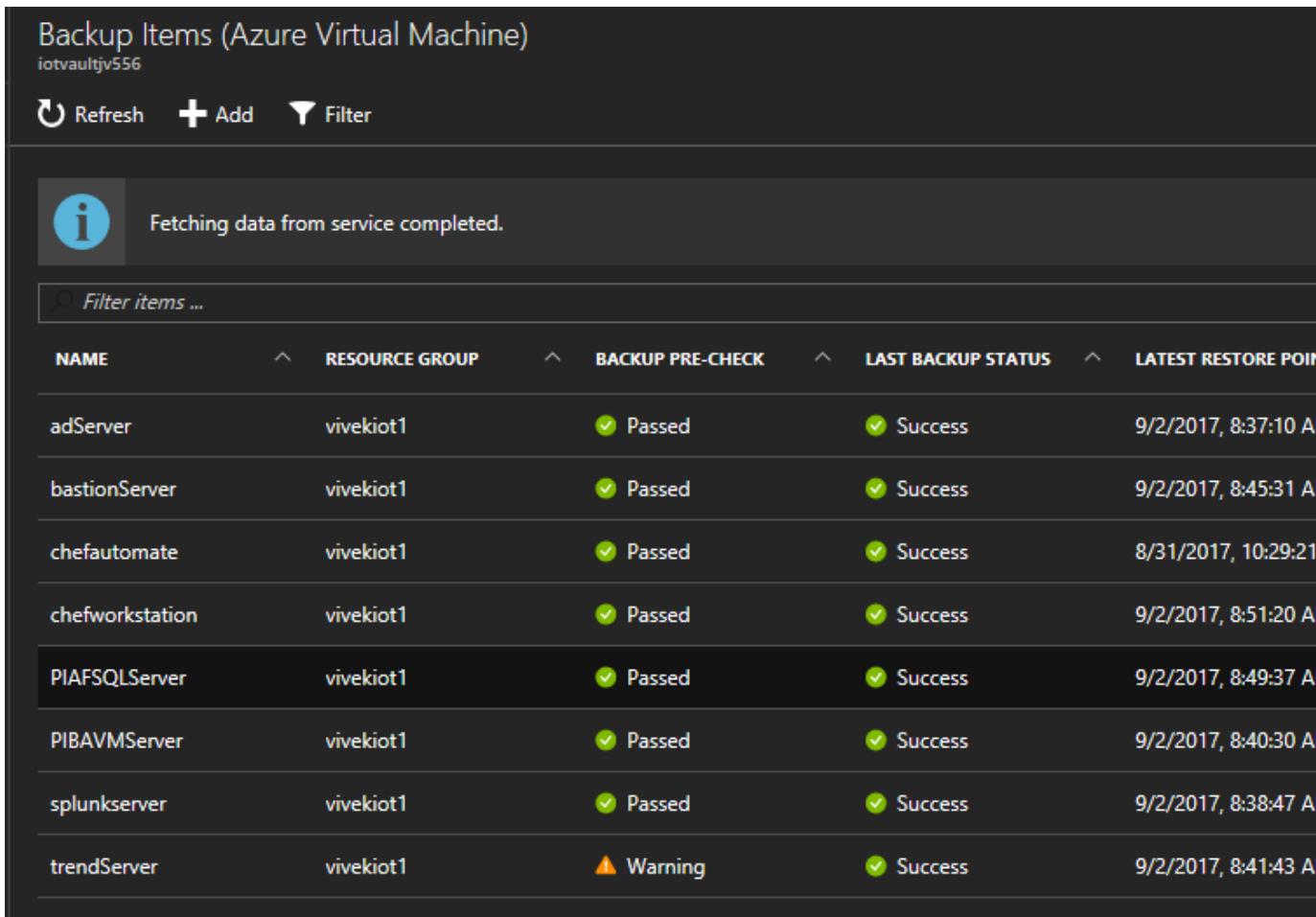
8



The screenshot shows the 'Backup Items' blade for an Azure Virtual Machine named 'vivekiot1'. The blade includes a header with 'Backup', 'Replicate', and 'Delete' buttons, a survey invitation, and a refresh button. Below the header is a summary section with details like Resource group, Status, Active, Location, Subscription name, and IOT Integration. The main area displays a table of backup items:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	8
Azure Backup Agent	0
Azure Backup Server	0

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



The screenshot shows the 'Backup Items (Azure Virtual Machine)' blade for a resource group named 'iotvaultjv556'. It includes a header with 'Refresh', 'Add', and 'Filter' buttons, a message indicating data fetching completion, and a search bar. The main table lists the following Azure virtual machines:

NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT
adServer	vivekiot1	Passed	Success	9/2/2017, 8:37:10 A
bastionServer	vivekiot1	Passed	Success	9/2/2017, 8:45:31 A
chefautomate	vivekiot1	Passed	Success	8/31/2017, 10:29:21
chefworkstation	vivekiot1	Passed	Success	9/2/2017, 8:51:20 A
PIAFSQLServer	vivekiot1	Passed	Success	9/2/2017, 8:49:37 A
PIBAVMServer	vivekiot1	Passed	Success	9/2/2017, 8:40:30 A
splunkserver	vivekiot1	Passed	Success	9/2/2017, 8:38:47 A
trendServer	vivekiot1	Warning	Success	9/2/2017, 8:41:43 A

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.

PIAFSQLServer
Backup Item

Settings **Backup now** **Restore VM** **File Recovery** **More**

Essentials ^

Recovery services vault	Last backup time
iotvaultazeqs	9/1/2017, 8:38:55 AM
Subscription name	Latest restore point
IOT Integration	9/1/2017, 8:38:58 AM (7 hour(s) ago)
Subscription ID	Oldest restore point
2927c217-b119-4d3b-8a13-82a1c3a16c8f	9/1/2017, 8:38:58 AM (7 hour(s) ago)
Item type	Backup policy
Azure virtual machine	iotpolicy
Last backup status	Backup Pre-Check
Success	Passed

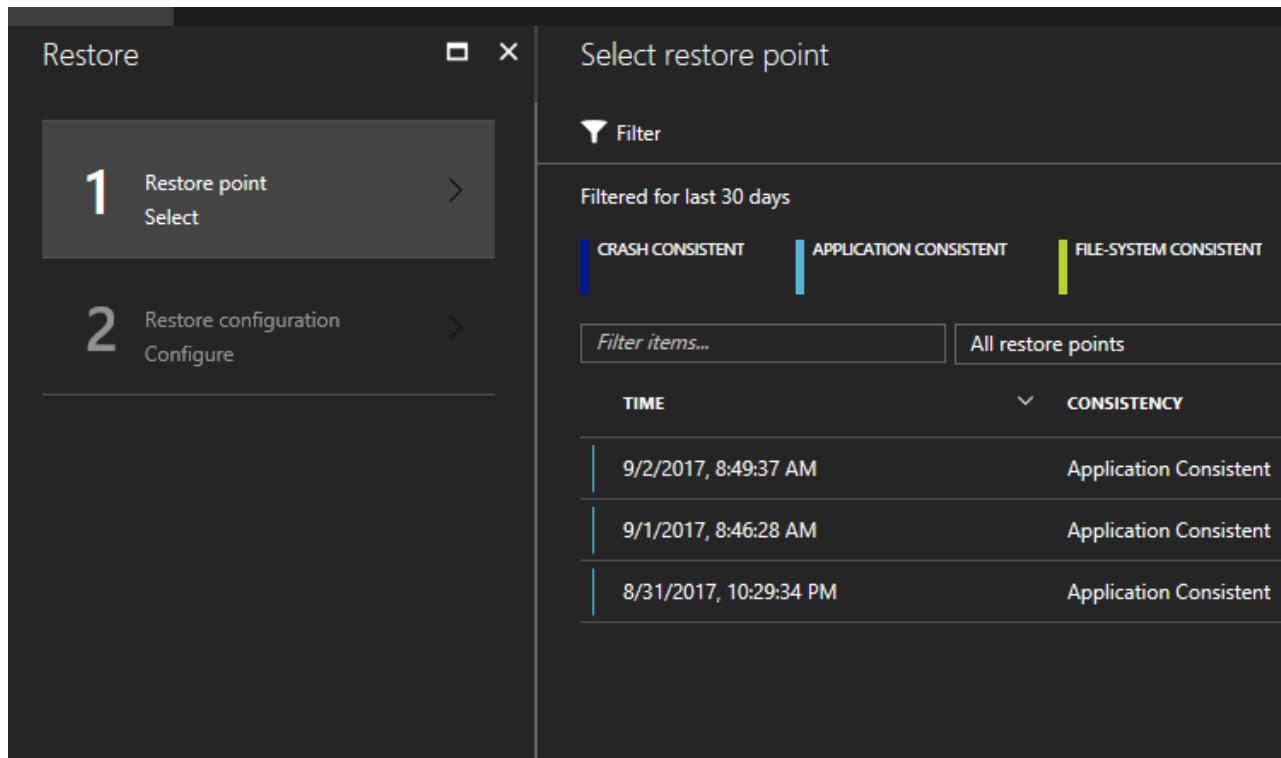
[All settings →](#)

Restore points

Restore points

Last 30 days	1
Last 7 days	1

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.

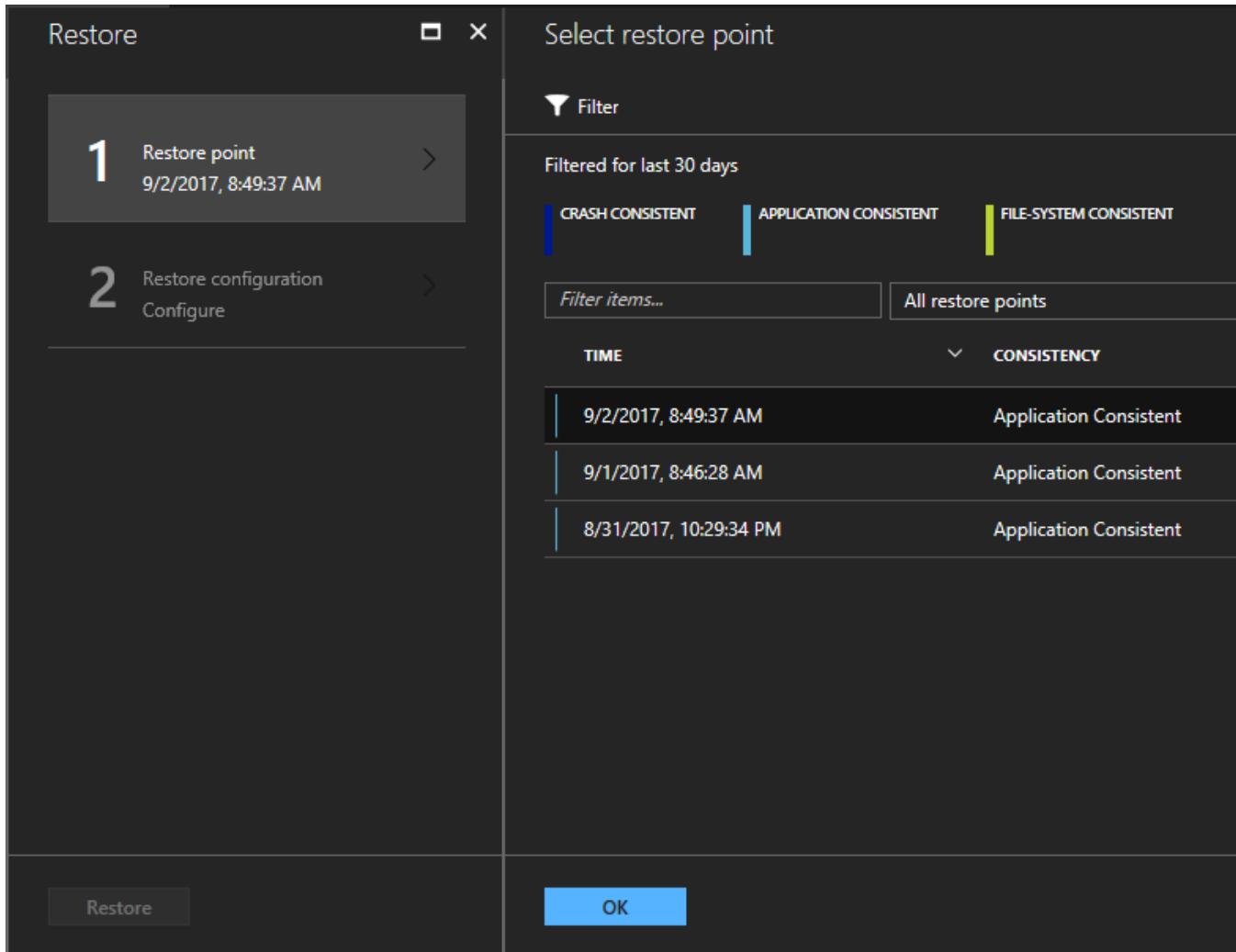


- By default, the dialog displays all restore points from the previous days. Use the **Filter** to alter the time range of the restore points displayed. By default, restore points of all consistency are displayed.

Restore point consistency from this list choose:

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

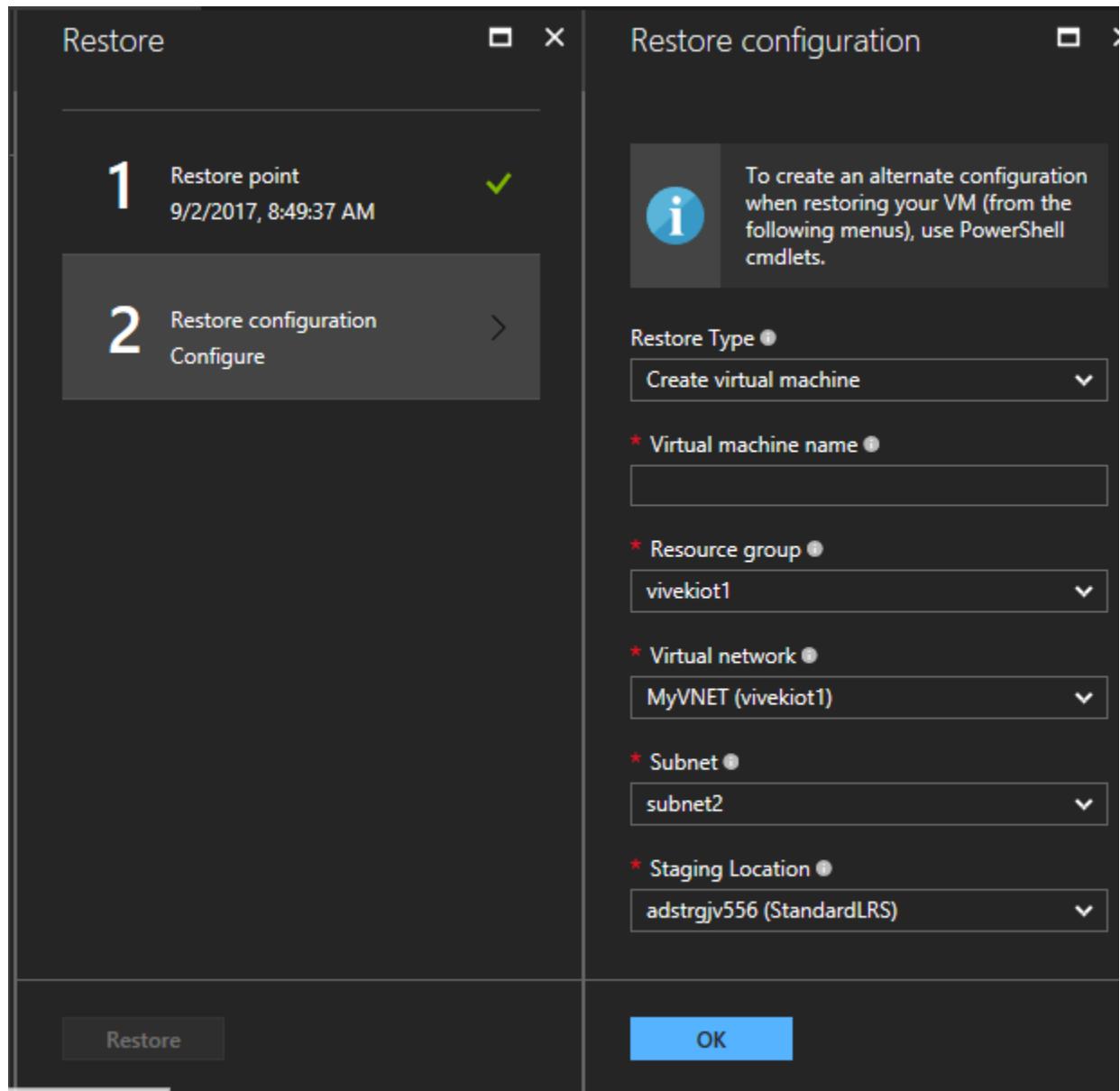
- Choose a Restore point and click OK.



The screenshot shows the Sysgain Restore blade. On the left, under 'Restore', a 'Restore point' is selected (9/2/2017, 8:49:37 AM). Below it, 'Restore configuration' is listed with a 'Configure' link. At the bottom are 'Restore' and 'OK' buttons. On the right, the 'Select restore point' panel is open, showing a list of restore points filtered for the last 30 days. The 'APPLICATION CONSISTENT' tab is selected. The list includes:

TIME	CONSISTENCY
9/2/2017, 8:49:37 AM	Application Consistent
9/1/2017, 8:46:28 AM	Application Consistent
8/31/2017, 10:29:34 PM	Application Consistent

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

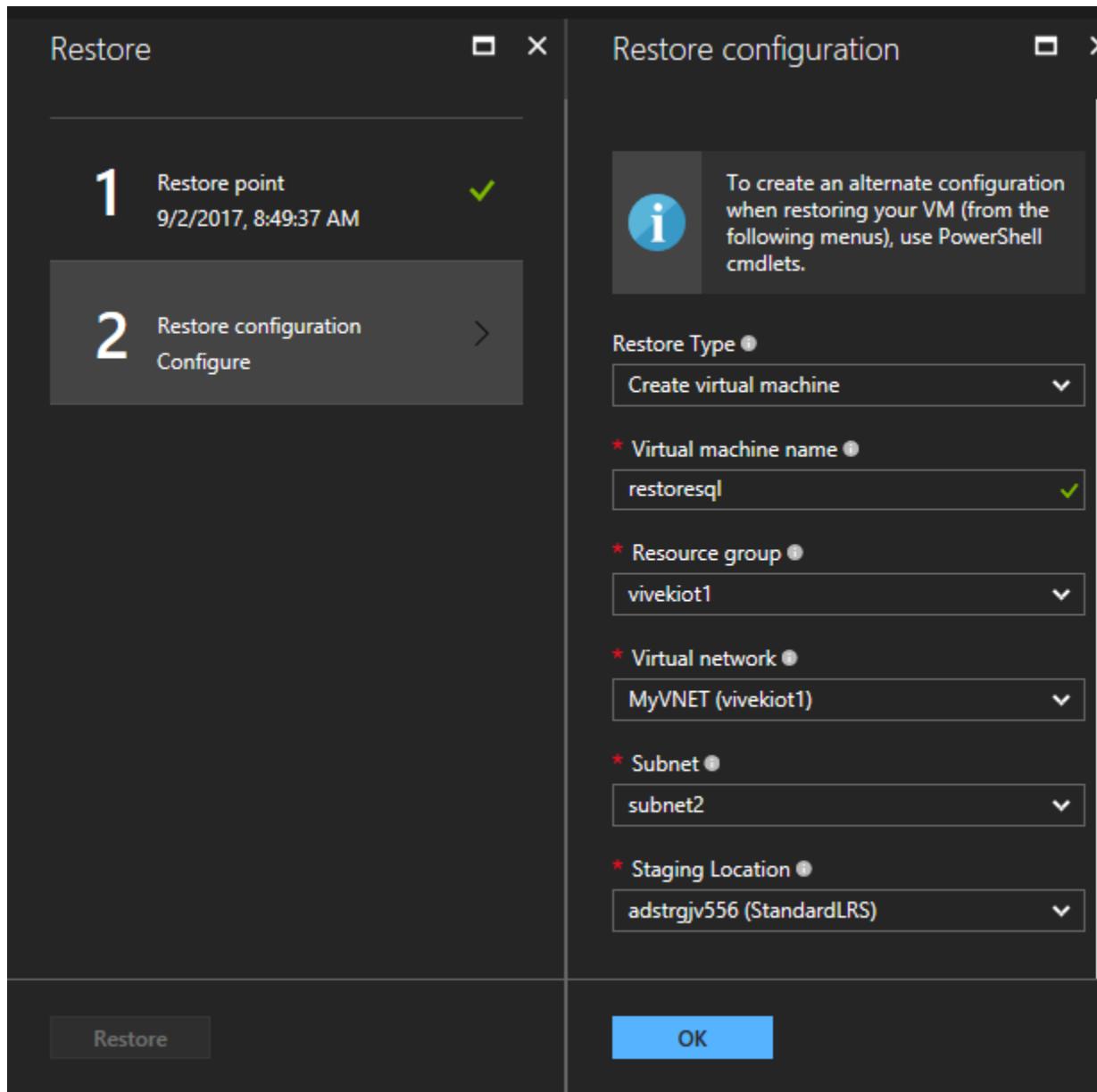
- Now that you have selected the restore point, choose a configuration for your restore VM.
- On the Restore configuration blade, you have two choices:
 - Restore full virtual machine
 - Restore backed up disks

14.2.1. Create a new VM from restore point

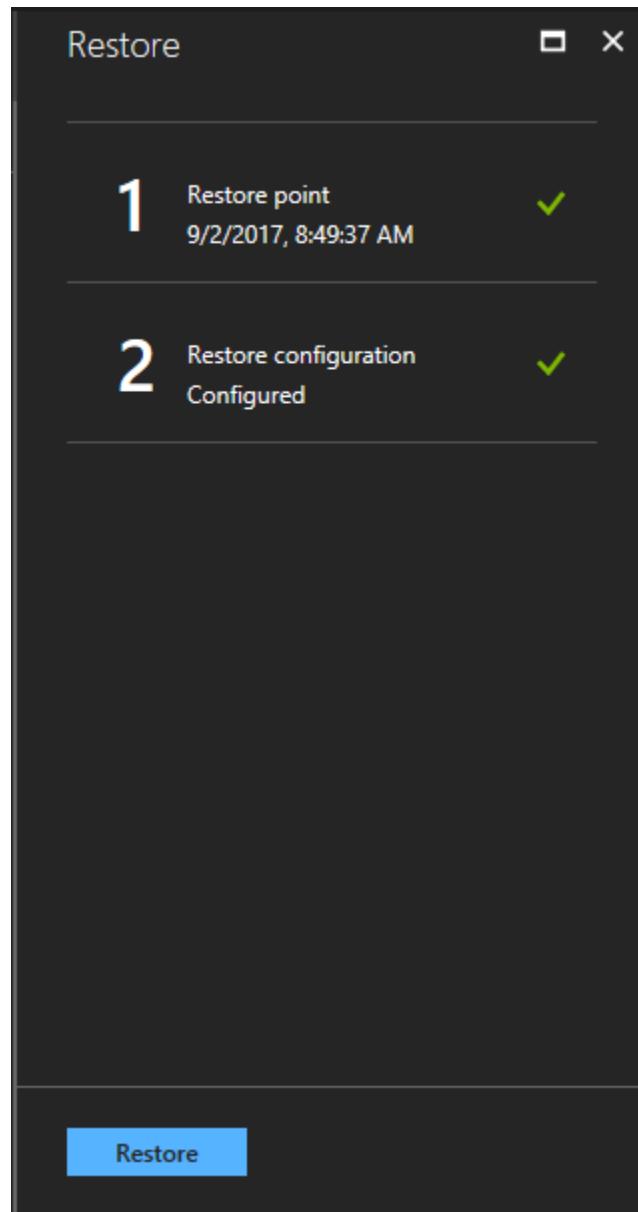
Select Restore Type as Create virtual machine.

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.

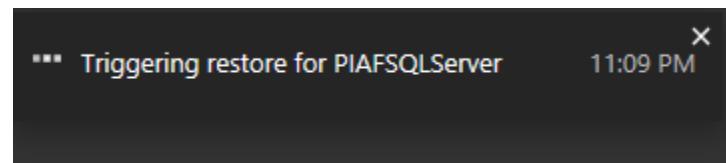


7. On the **Restore configuration** blade, click **OK** to finalize the restore configuration.
8. On the **Restore** blade, click **Restore** to trigger the restore operation.



14.3. Track the restore operation

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

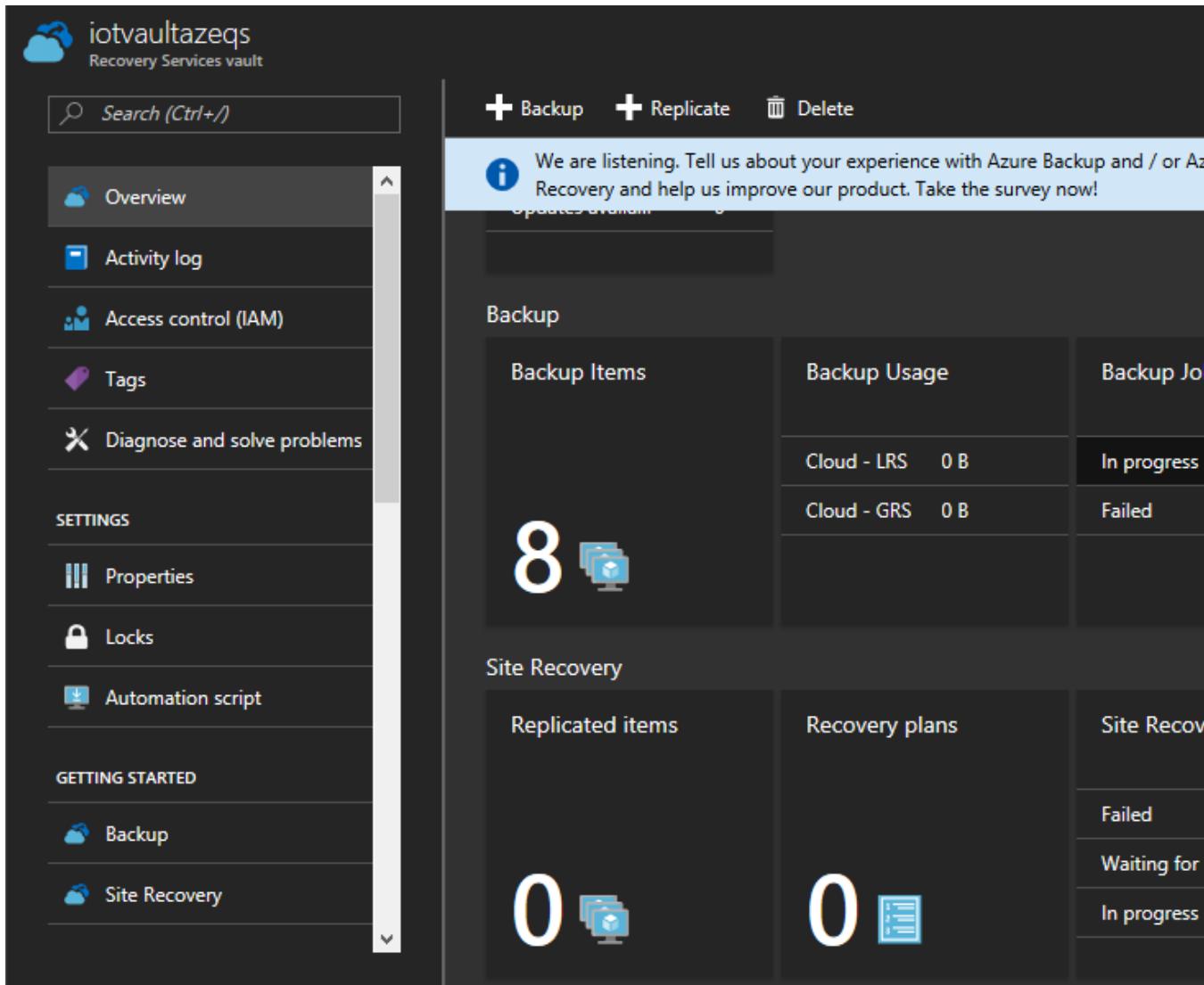


Notifications

Dismiss: Informational Completed All

✓ Triggering restore for PIAFSQLServer 4:46 PM
Restore triggered successfully. Please monitor progress in backup jobs page.

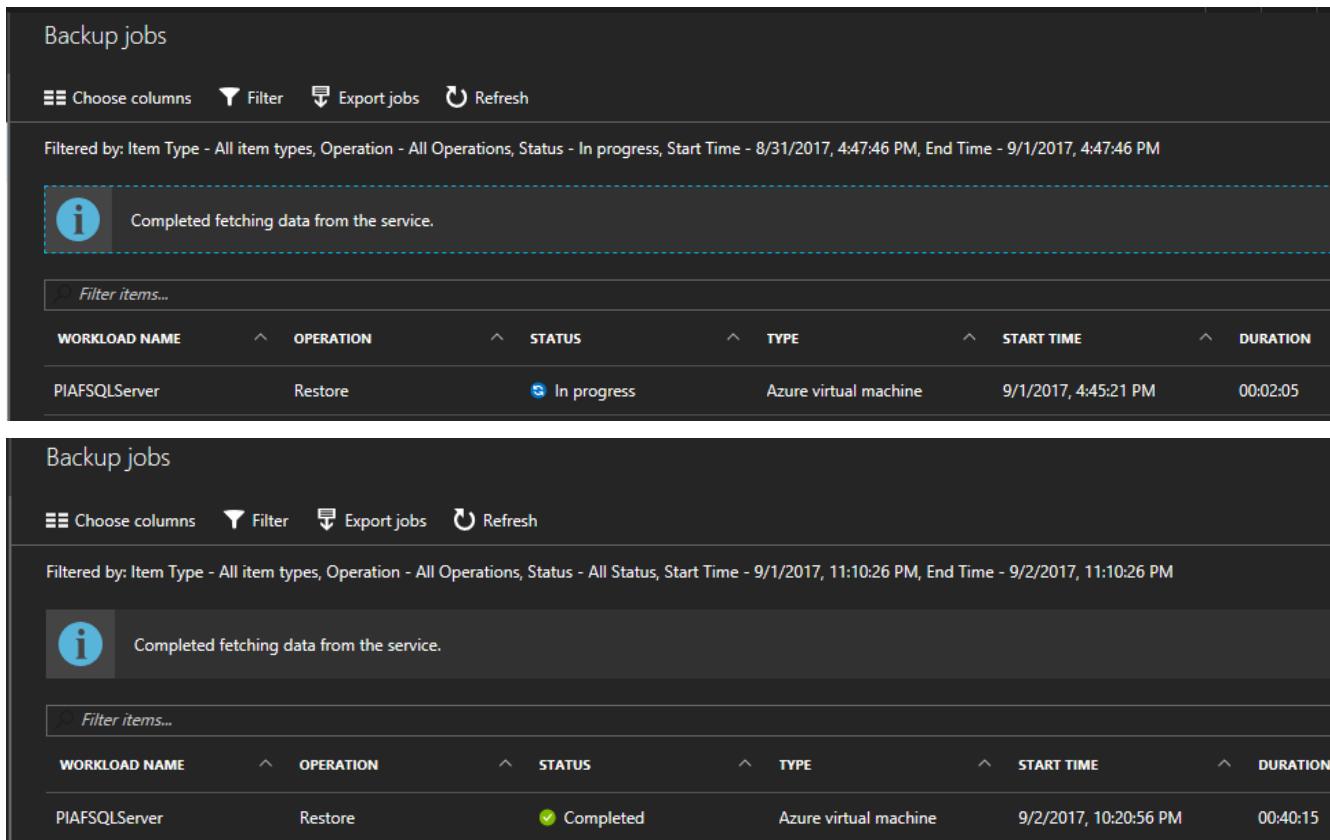
2. To view the operation while it is processing, or to view when it completed, open the Backup jobs list.
3. In the vault dashboard on the **Backup Jobs** tile, click **Azure Virtual Machines** to display the jobs associated with the vault.



The screenshot shows the Azure Recovery Services vault dashboard for the vault 'iotvaultazeqs'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, and Automation script. Under SETTINGS, there are links for Backup and Site Recovery. The main content area has tabs for Backup, Site Recovery, and Recovery Services. The Backup tab displays 8 backup items, 0 B of Cloud - LRS usage, and 0 B of Cloud - GRS usage. The Site Recovery tab shows 0 replicated items and 0 recovery plans. A survey prompt is visible in the center of the dashboard.

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

8



The screenshot shows two separate instances of the 'Backup jobs' blade. Both instances display a table with columns: WORKLOAD NAME, OPERATION, STATUS, TYPE, START TIME, and DURATION. In the first instance, the status is 'In progress'. In the second instance, the status is 'Completed'. Both instances show a single row for 'PIAFSQLServer' with a restore operation.

WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION
PIAFSQLServer	Restore	In progress	Azure virtual machine	9/1/2017, 4:45:21 PM	00:02:05

WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION
PIAFSQLServer	Restore	Completed	Azure virtual machine	9/2/2017, 10:20:56 PM	00:40:15

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



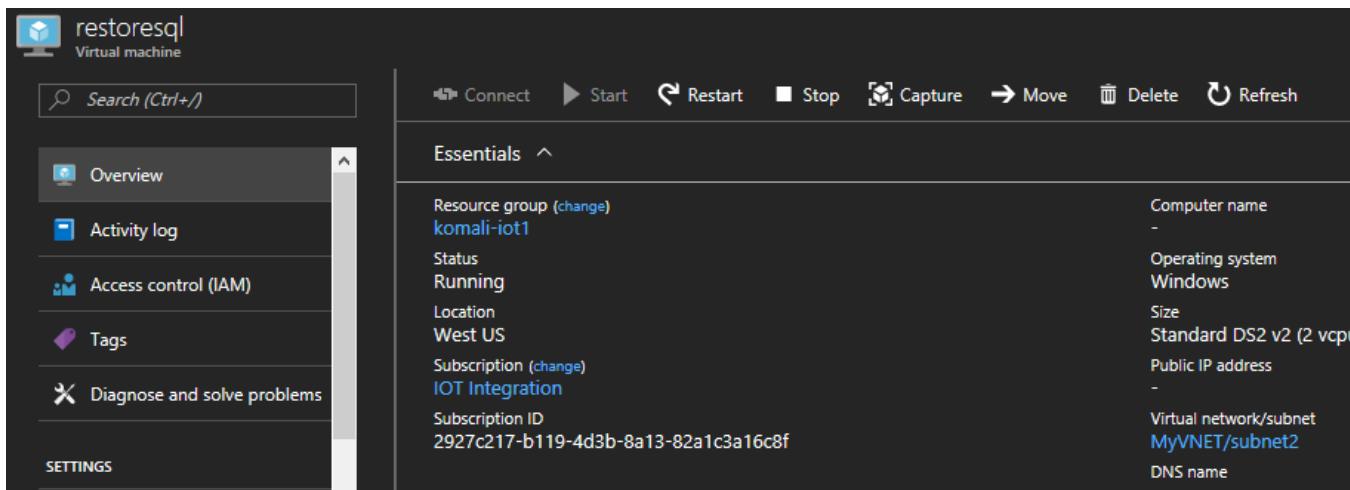
The screenshot shows the 'Resource Groups' blade with a list of virtual machines. The machines listed are: chefautomate, chefworkstation, fortigate, PIAFSQLServer, PIBAVMServer, restoresql, splunkserver, and trendServer. All are categorized as Virtual machines and located in West US. Each item has a three-dot menu icon on the far right.

 chefautomate	Virtual machine	West US	...
 chefworkstation	Virtual machine	West US	...
 fortigate	Virtual machine	West US	...
 PIAFSQLServer	Virtual machine	West US	...
 PIBAVMServer	Virtual machine	West US	...
 restoresql	Virtual machine	West US	...
 splunkserver	Virtual machine	West US	...
 trendServer	Virtual machine	West US	...

274

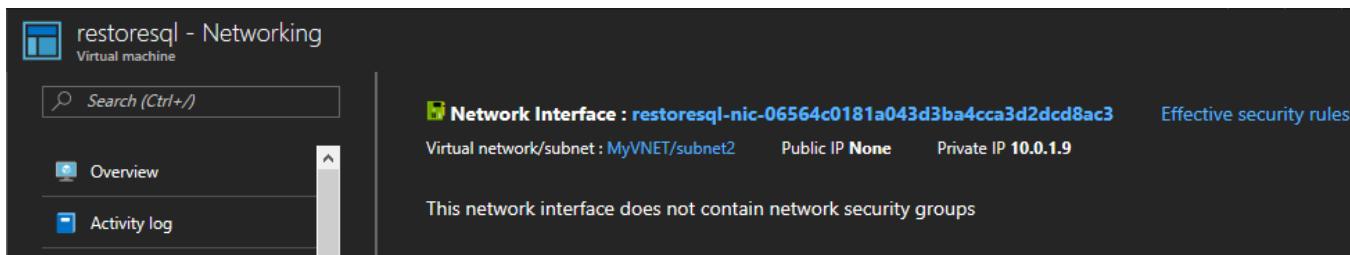
Post-Restore steps

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.



Setting	Value
Computer name	-
Operating system	Windows
Size	Standard DS2 v2 (2 vcpus)
Public IP address	-
Virtual network/subnet	MyVNET/subnet2
DNS name	-

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

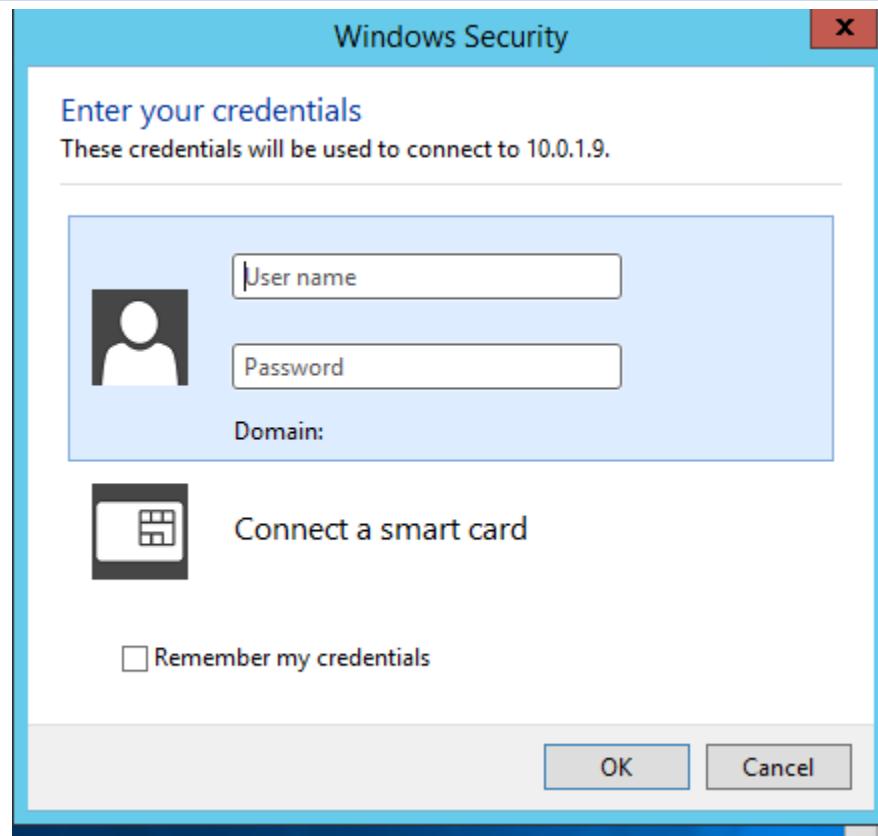


Network Interface : restoresql-nic-06564c0181a043d3ba4cca3d2dcd8ac3

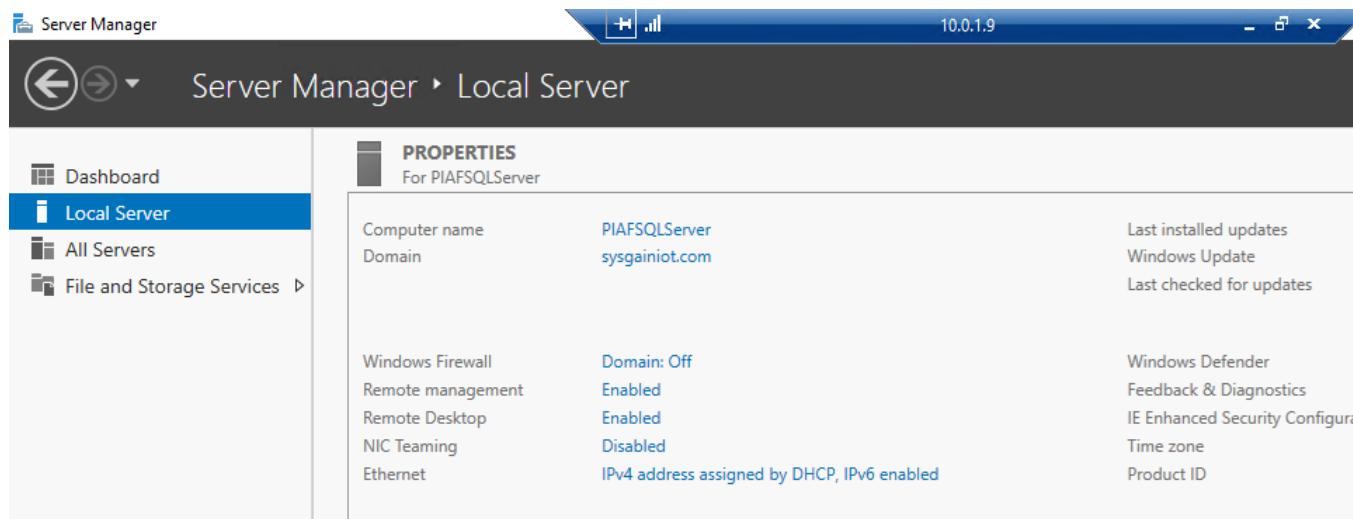
Virtual network/subnet : MyVNET/subnet2 Public IP None Private IP 10.0.1.9

This network interface does not contain network security groups

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



8



The screenshot shows the "Server Manager" interface with the title bar "Server Manager" and IP address "10.0.1.9". The left navigation pane shows "Local Server" selected under "All Servers". The main content area displays the "PROPERTIES" for the server "PIAFSQLServer". The properties listed include:

Computer name	PIAFSQLServer	Last installed updates
Domain	sysgainiot.com	Windows Update
Windows Firewall	Domain: Off	Last checked for updates
Remote management	Enabled	Windows Defender
Remote Desktop	Enabled	Feedback & Diagnostics
NIC Teaming	Disabled	IE Enhanced Security Configuration
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Time zone
		Product ID

bastionServer-1 - 13.88.26.183:3389 - Remote Desktop Connection

SQLQuery3.sql - sqlserver4c7xh.database.windows.net.azuredb (sqluser) 10.0.1.9

File Edit View Query Project Debug Tools Window Help

New Query Execute Debug Generic Debugger

azuredb

Object Explorer

```
SQLQuery3.sql - sql...redb (sqluser (101)) SQLQuery2.sql - sql...uredb (sqluser (98)) SQLQuery1.sql - sql...uredb (sqluser (98))
***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [Id]
    ,[AMPS_L1]
    ,[AMPS_L2]
    ,[AMPS_L3]
    ,[AMPS_SYSTEM_AVG]
    ,[Breaker_details]
    ,[Breaker_label]
    ,[Building]
    ,[ClassOccupanyRemaining]
    ,[ClassOccupiedValue]
    ,[TotalClassCapacity]
    ,[Daily_electric_cost]
    ,[Daily_KWH_System]
    ,[isClassOccupied]
    ,[KW_L1]
    ,[KW_L2]
```

Results Messages

	Id	AMPS_L1	AMPS_L2	AMPS_L3	AMPS_SYSTEM_AVG	Breaker_details
1	1	50.6454135542511	51.2469971504382	51.002419219025	51.002419219025	New (2013) 3rd floor panel - almost emp
2	2	69.3024981644668	70.1256970119966	69.7910198822566	69.7910198822566	New (2013) 4th floor panel - almost emp
3	3	108.796504197208	110.088826396877	109.563423955192	109.563423955192	New (2018) 4th floor panel - almost emp
4	4	67.8138422158681	68.6193582973547	68.2918702172629	68.2918702172629	New (2013) 3rd floor panel - almost emp
5	5	71.1518101662343	71.9969757761305	71.6533679086951	71.6533679086951	New (2013) 4th floor panel - almost emp
6	6	110.19703573853	111.5059939323	110.973828013269	110.973828013269	New (2018) 4th floor panel - almost emp
7	7	70.3289157499257	71.1643067376498	70.8246728098071	70.0591480335381	New (2013) 3rd floor panel - almost emp
8	8	67.0645549558174	67.8611707461849	67.5373011404077	67.5373011404077	New (2013) 4th floor panel - almost emp
9	9	117.80439541763	119.203716439385	118.634812893722	118.634812893722	New (2018) 4th floor panel - almost emp
10	10	56.4886592177897	57.159650890503	56.8868546301863	56.8868546301863	New (2013) 3rd floor panel - almost emp

- 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.

