



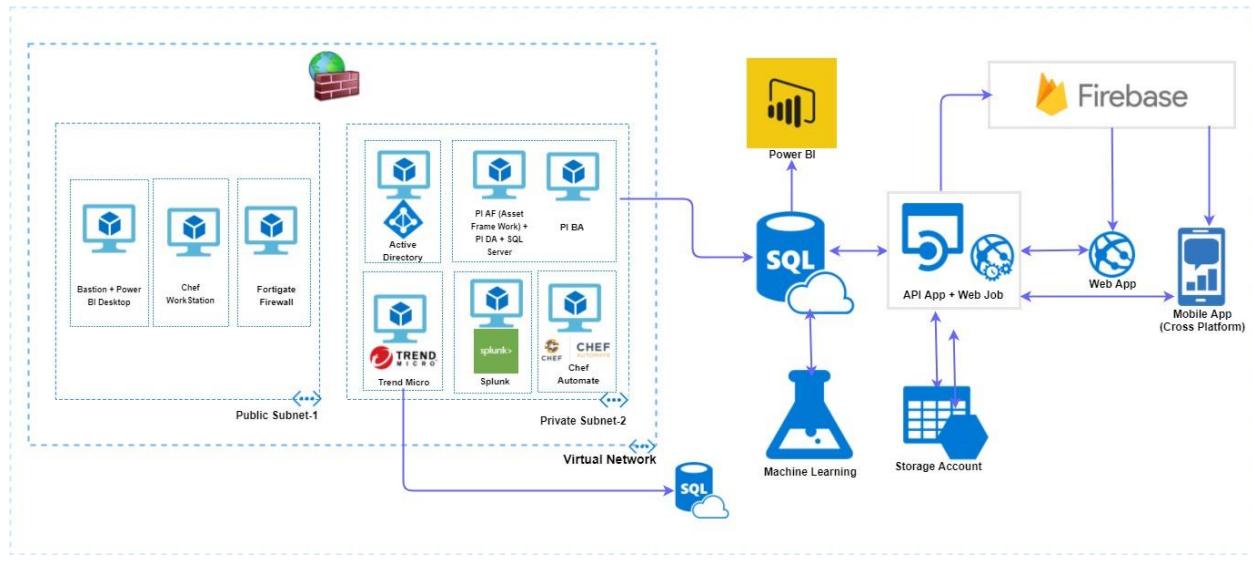
Internet of Things Automation User Guide

Contents

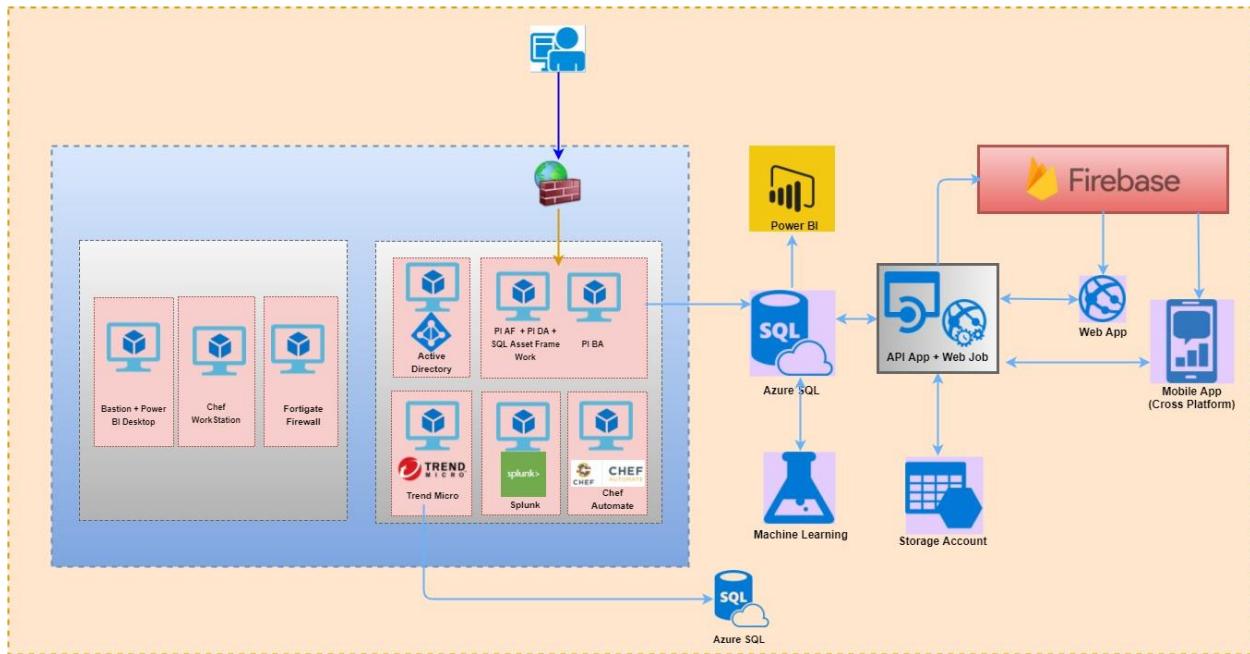
1. Architecture	4
1.1. Data Flow Architecture Diagram	5
2. High Level Deployment Process to be Followed.....	5
3. Deployment Costs	6
3.1. SERVER DETAILS	8
4. Prerequisites.....	8
4.1 Launching Firewall Template	8
4.2. Azure B2C Tenant Creation and Configuration.....	22
4.3. Power BI Configuration.....	41
4.4. Dynatrace Account Creation (If You Don't Have an Existing Account)	47
5. Input Parameters	51
6. Azure Resource Manager Template Deployment	55
6.1. Output Parameters.....	60
7. Security and Monitoring Components.....	63
7.1. Dynatrace	64
7.1.1. Installing Dynatraceoneagent To Web Application (PaaS Environment).....	75
7.2. Chef Automate.....	86
7.3. Splunk	90
7.4. TrendMicro	93
8. Create User for PI Business Analytics (PIBA) Interface.....	108
8.1. Create PIBA User in PIAF Server.....	118
8.2. Enable TCP and Named Pipe in SQL Server Configuration Management.....	125
9. Components of PI Server.....	128
9.1. PI Asset FrameWork (AF)	128
9.1.1. Installation of PIAF Server	128
9.2. PI Data Archive (PIDA)	131
9.2.1. Installation of Data Archive (PIDA)	132

9.3. PI Web API Utility	141
9.4. Creation of Database in PI System Explorer	148
9.5. System Configuration in PI System Explorer	151
9.6. Import .XML Files into AF Server.....	155
9.7. Update Security in PI System Management Tools.....	163
9.8. Prepare Data Server for Module Database(MDB) To Asset Framework(AF)	177
9.9. Update PI Points in PI System Explorer.....	182
9.10. Install and Run The Piweb Simulator Setup	186
10. Installation of PI BA Integrator	193
10.1. Configuring PI Business Analytics	200
10.2. Install And Run The DataServiceAppSetup	220
11. Configuring and Accessing the Webapp	245
12. Machine Learning Experiment	251
13. Firebase Configuration	263
14. Restore Virtual Machines	268
14.1. Select restore point for restore	268
14.2. Choosing a VM restore configuration.....	275
14.2.1. Create a new VM from restore point.....	276
14.3. Track the restore operation.....	278

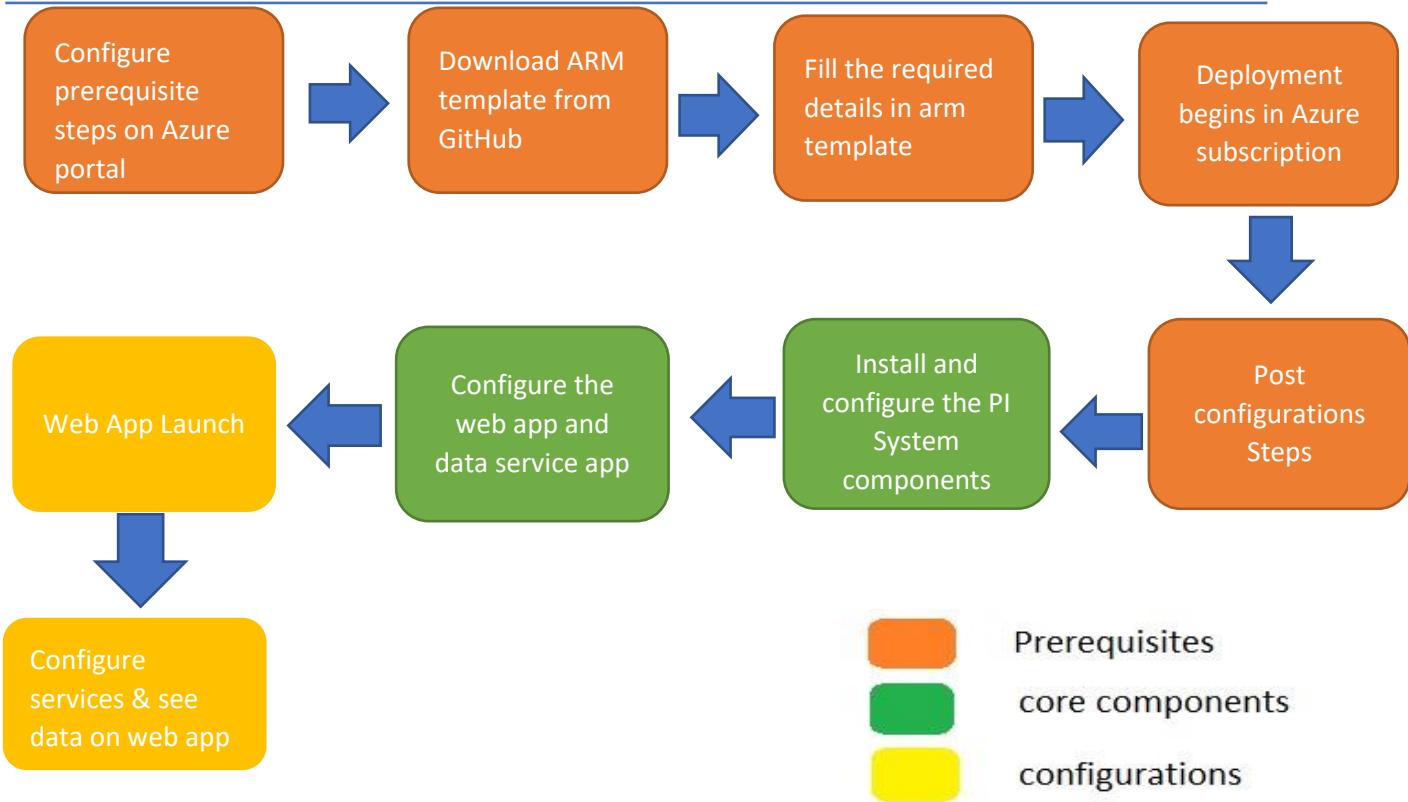
1. Architecture



1.1. Data Flow Architecture Diagram



2. High Level Deployment Process to be Followed



3. Deployment Costs

VM Name	VMSize	OS	Software Cost	Azure Cost/Hour	Azure Cost/Month
Bastion Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2012 R2	PAYG	\$ 0.21/Hour	\$98.95/Month
Chef Automate Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL (license \$137node/annual)	\$ 0.14/Hour	\$197.90/Month
Active Directory Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2016	PAYG	\$ 0.21/Hour	\$197.90/Month

Chef workstation	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2012 R2	PAYG	\$ 0.21/Hour	\$197.90/Month
PIAFSQL Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2016 + SQL 2016SP1	BYOL	\$0.61/Hour	\$98.95 /Month
PIBAVM Server	Standard DS4 v2 (8 cores, 28 GB memory)	Windows 2012 R2	BYOL	\$ 0.84/Hour	\$790.87/Month
Splunk Server	Standard DS2 v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	\$ 0.14/Hour	\$159.22/Month
Trend Micro	Standard DS2 v2 (2 cores, 7 GB memory)	CentOS 7	BYOL	\$ 0.14/Hour	\$159.22/Month
Web App	S1 Standard (1 instance)			\$ 0.1/Hour	\$279.74/Month
API App	S1 Standard (1 instance)			\$ 0.1/Hour	\$279.74/Month
FortiGate Firewall	Standard D2 v2 (2 core, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	\$ 0.14/Hour	\$104.16/Month
Machine Learning	S1 Standard			\$1 per studio experimentation/hour	\$9.99 per seat/month

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

3.1. SERVER DETAILS

S.NO	Server Name	Abbreviation	Purpose
1	PIAFSQL Server	PI Assert Framework	On this server we will install ULF Connector, AF Server, DA Server
2	PIBA Server	PI Business Analytics	On this server we install BA Installation and config PIBAVM Server
3	Chef Automate	Chef Automate	It provides a dashboard which is used to view all nodes and compliance of the nodes, In this we run chef automate
4	Chef Workstation	Chef Workstation	User will user to bootstrap, managing and applying cookbooks to all the nodes
5	PIDA Server	PI Data Archive	This installation we do in PIAFSQL Server

4. Prerequisites

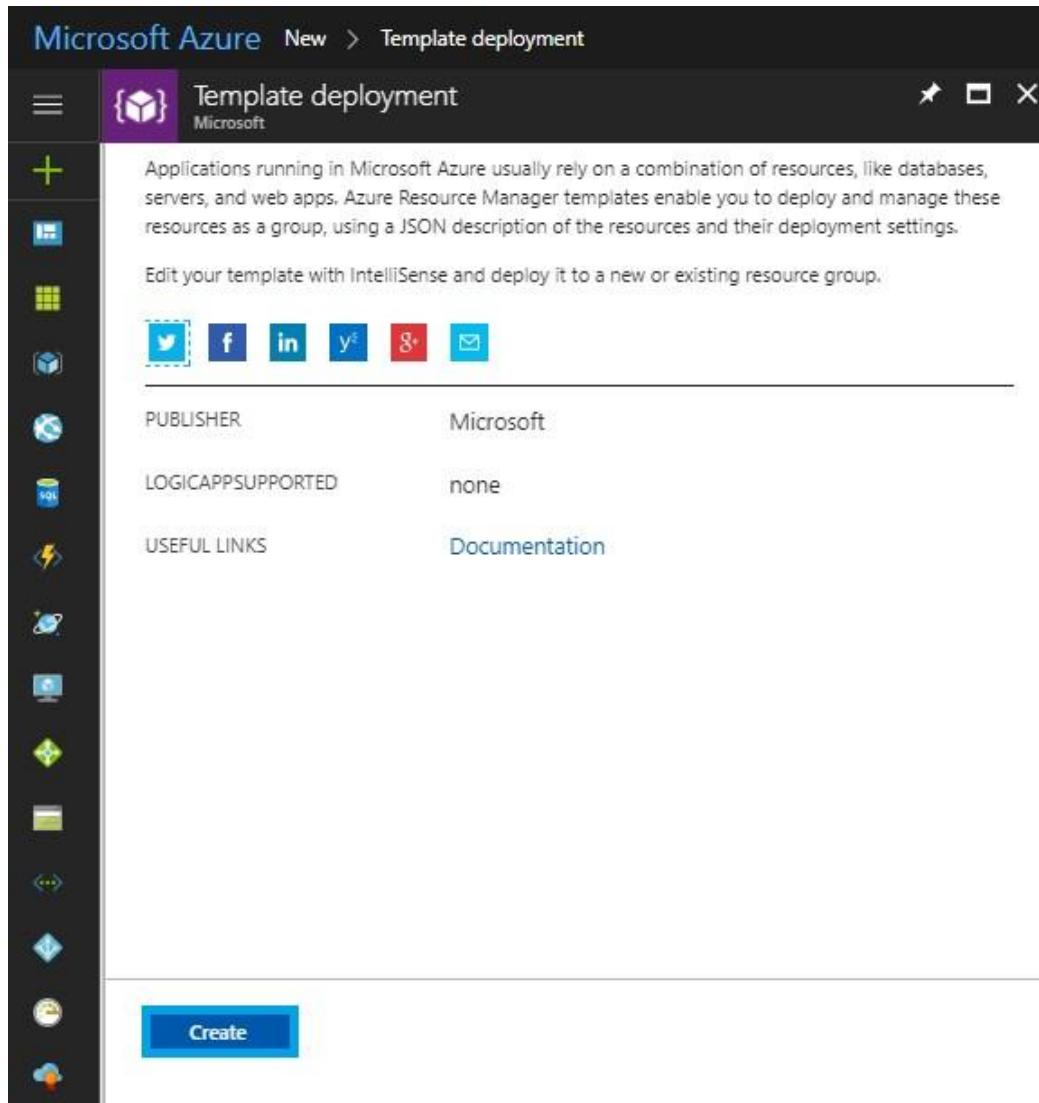
1. Launching Firewall Template
2. The Azure AD B2C Tenant should be created and register your web application.
3. Create an account in Power BI.
4. Dynatrace account creation in SAAS.

4.1 Launching Firewall Template

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

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

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



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

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](#)

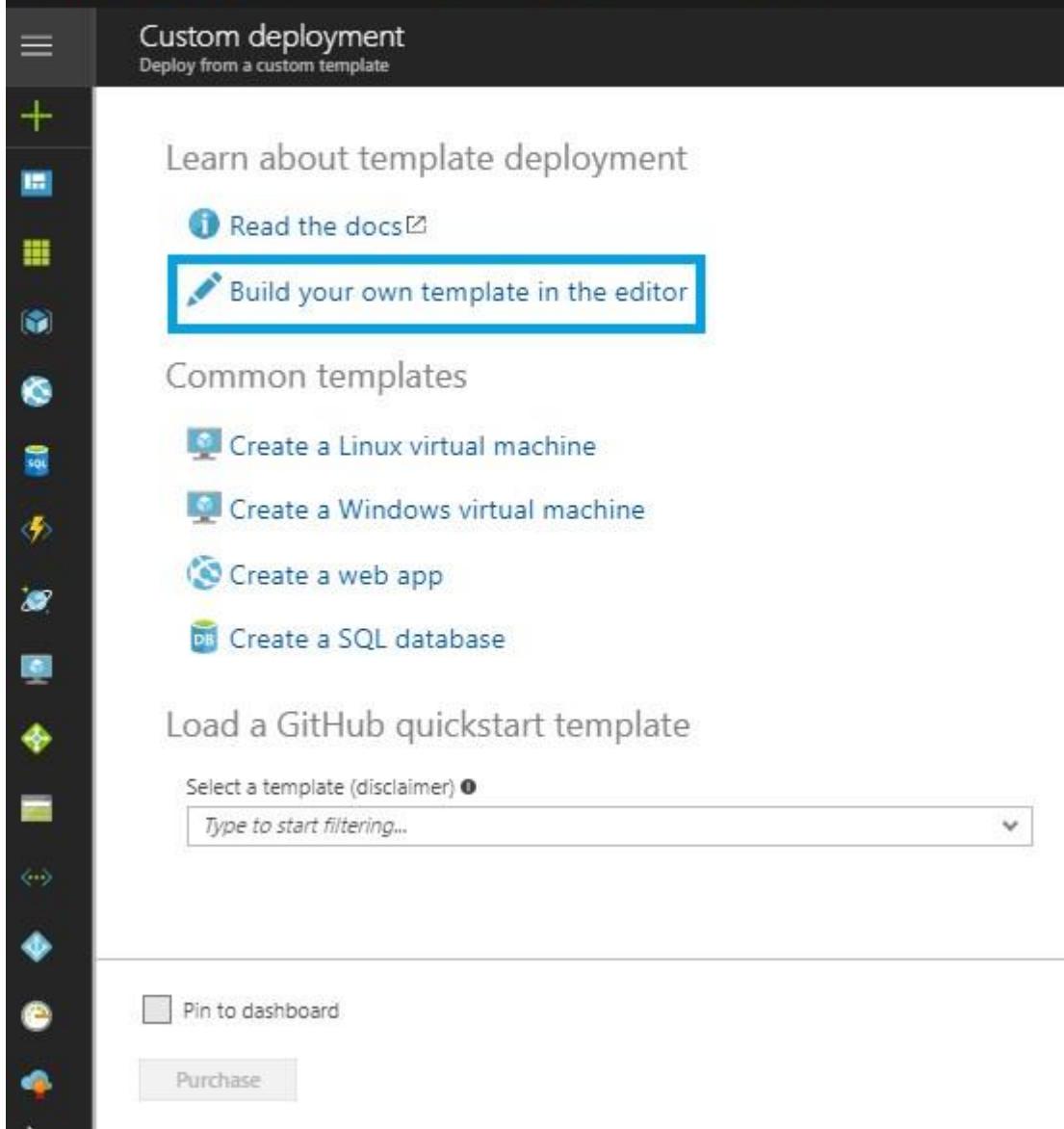
Load a GitHub quickstart template

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 your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↲ Load file ↴ Download

- Parameters (3)
- Variables (9)
- Resources (4)
 - [variables('fortigateFirewallSetting...')
 - [variables('fortigateFirewallSetting...')
 - [variables('networkSettings').virtua...]
 - 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,n
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 }
```

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 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.

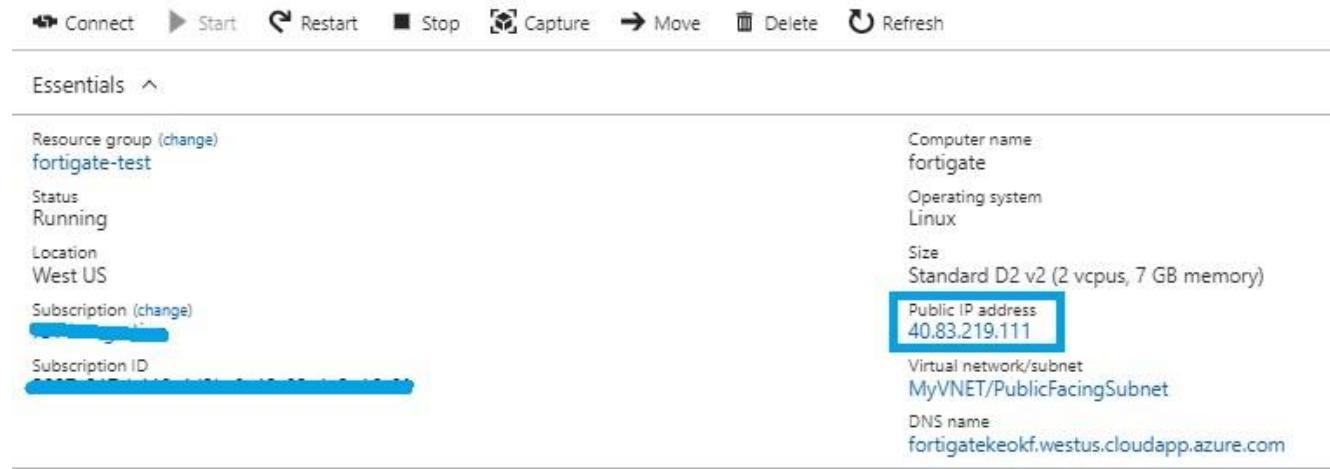
If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

I agree to the terms and conditions stated above

Pin to dashboard

Purchase

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



The screenshot shows the Azure portal interface for a virtual machine named 'fortigate-test'. The 'Essentials' section displays basic information: Resource group (fortigate-test), Status (Running), Location (West US), and Subscription (redacted). On the right, detailed properties are listed: Computer name (fortigate), Operating system (Linux), Size (Standard D2 v2 (2 vcpus, 7 GB memory)), and DNS name (fortigatekeokf.westus.cloudapp.azure.com). The 'Public IP address' field, containing '40.83.219.111', is highlighted with a blue box.

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)	[REDACTED]	Public IP address	40.83.219.111
Subscription ID	[REDACTED]	Virtual network/subnet	MyVNET/PublicFacingSubnet
		DNS name	fortigatekeokf.westus.cloudapp.azure.com

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



Not secure <https://40.83.219.111>

System Dashboard - Microsoft Office Home Mail - sushmithan@sysgain.com Dashboard - Microsoft



Your connection is not private

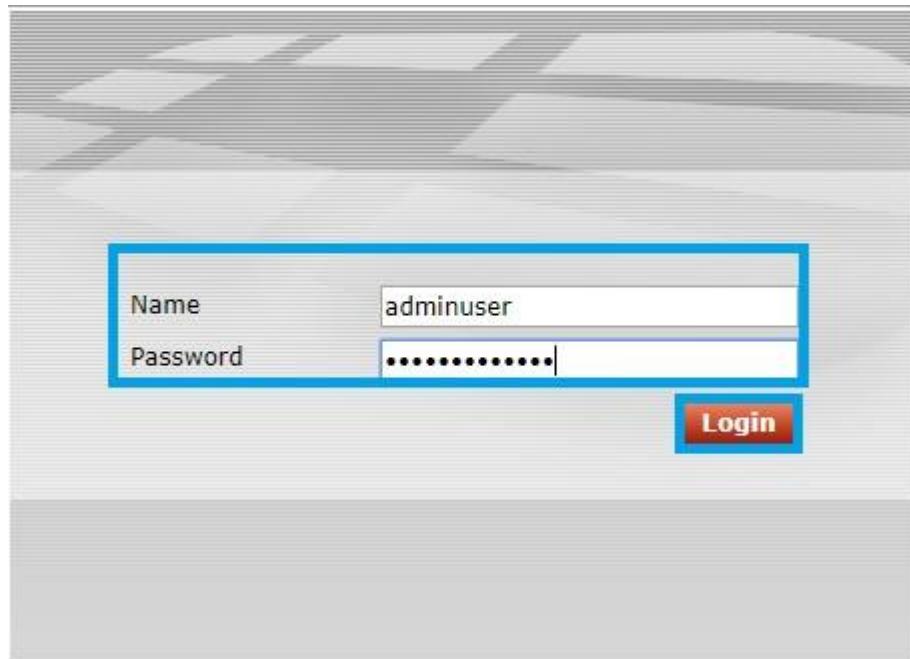
Attackers might be trying to steal your information from **40.83.219.111** (for example, passwords, messages, or credit cards). [Learn more](#)
NET::ERR_CERT_AUTHORITY_INVALID

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.



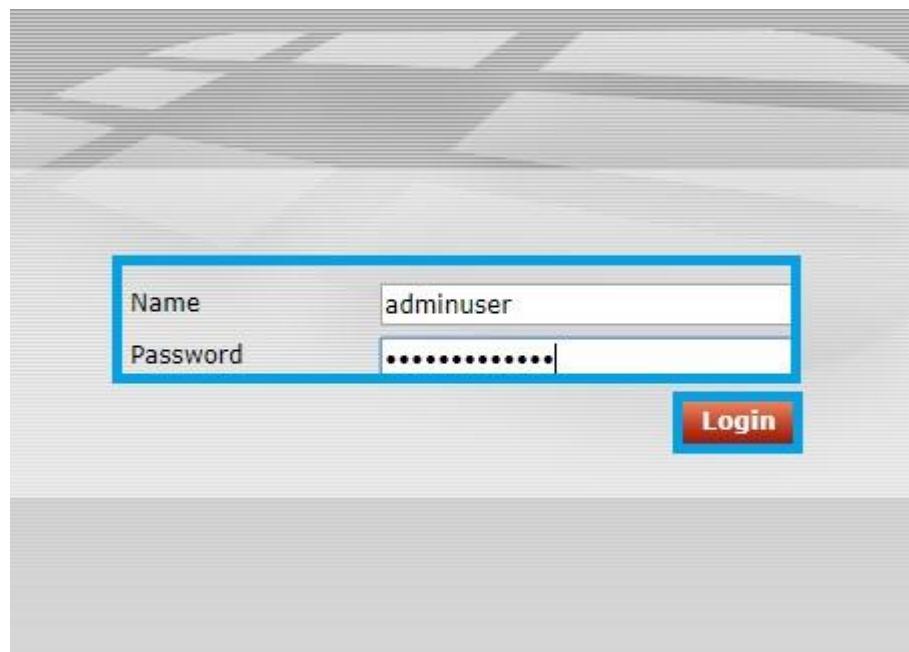
9. After logging in, you will see the "Install Fortigate-VM License File" page. If you already have the fortigate license file from Fortigate , click the "Choose File" button and navigate to that file in the dialogue box and appears. If you don't have the license file, contact Fortigate Support at <https://support.fortinet.com>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



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

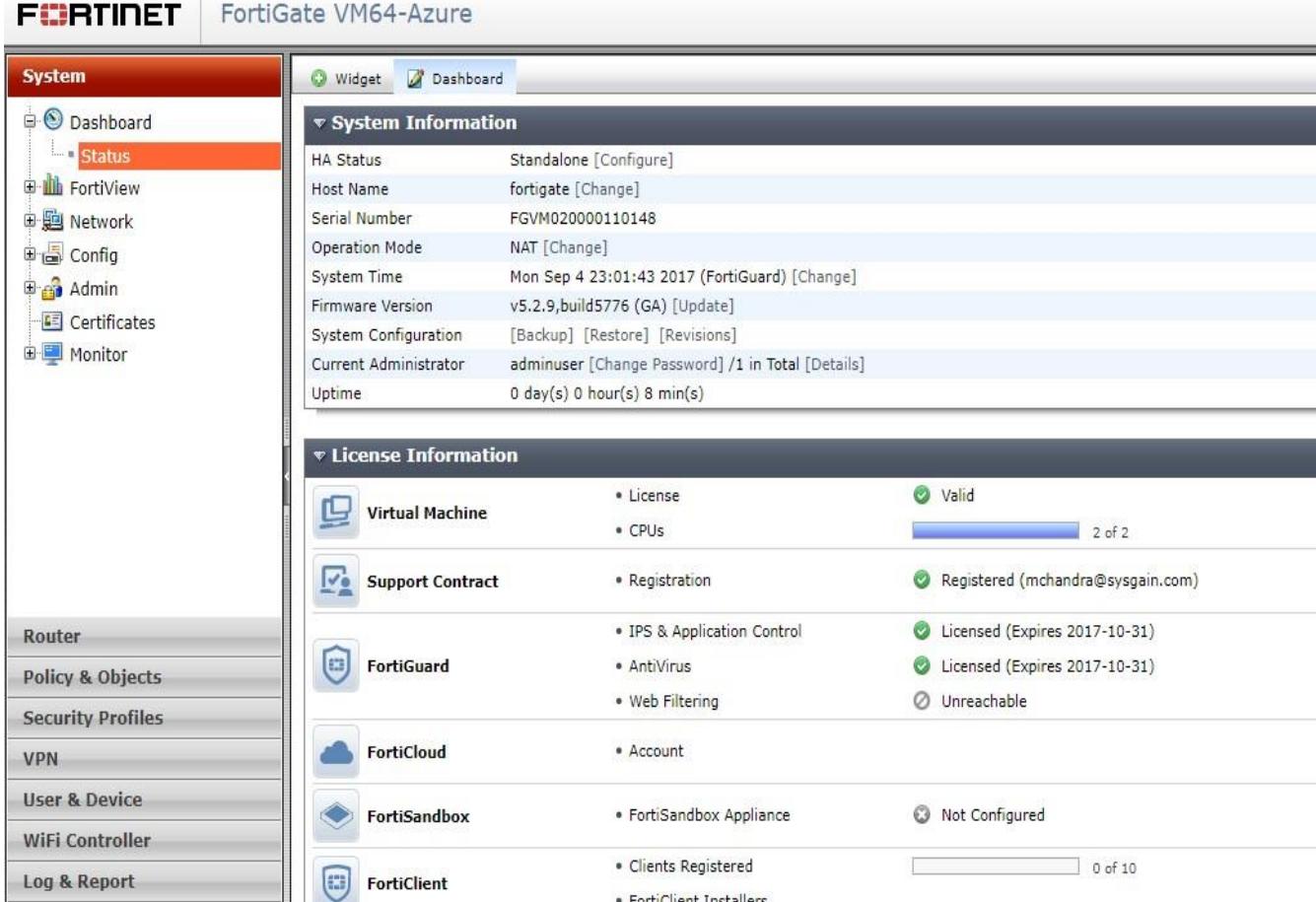
Please wait while system restarts.

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.

FORTINET FortiGate VM64-Azure



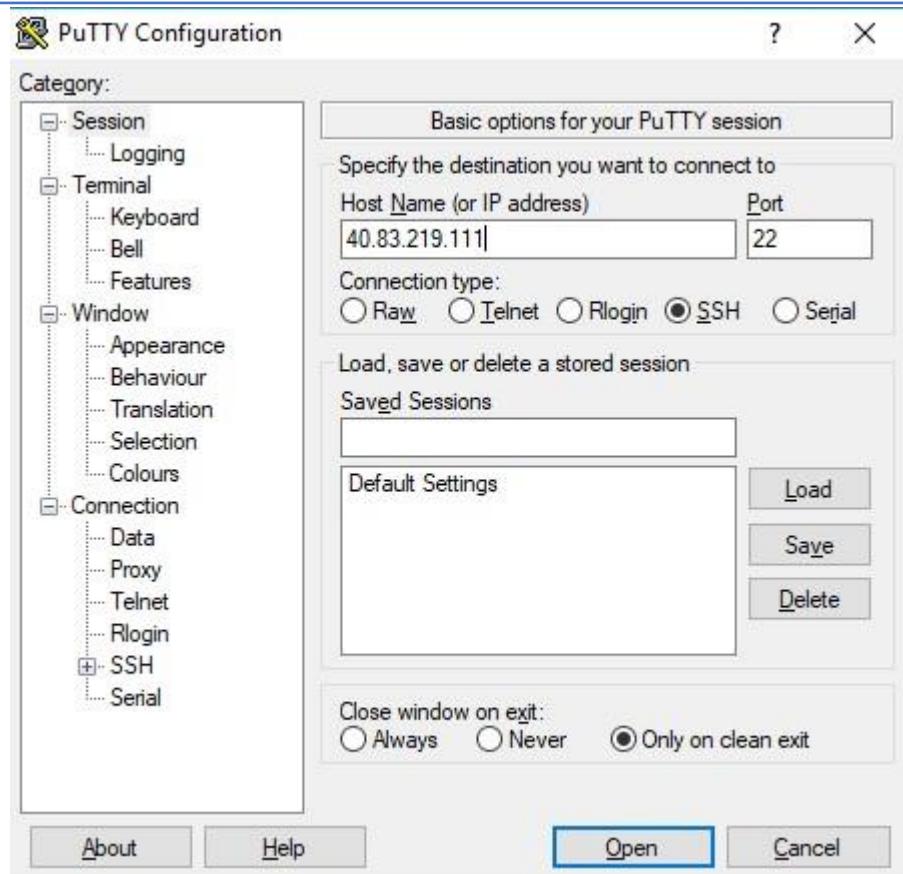
System Information

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

- 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

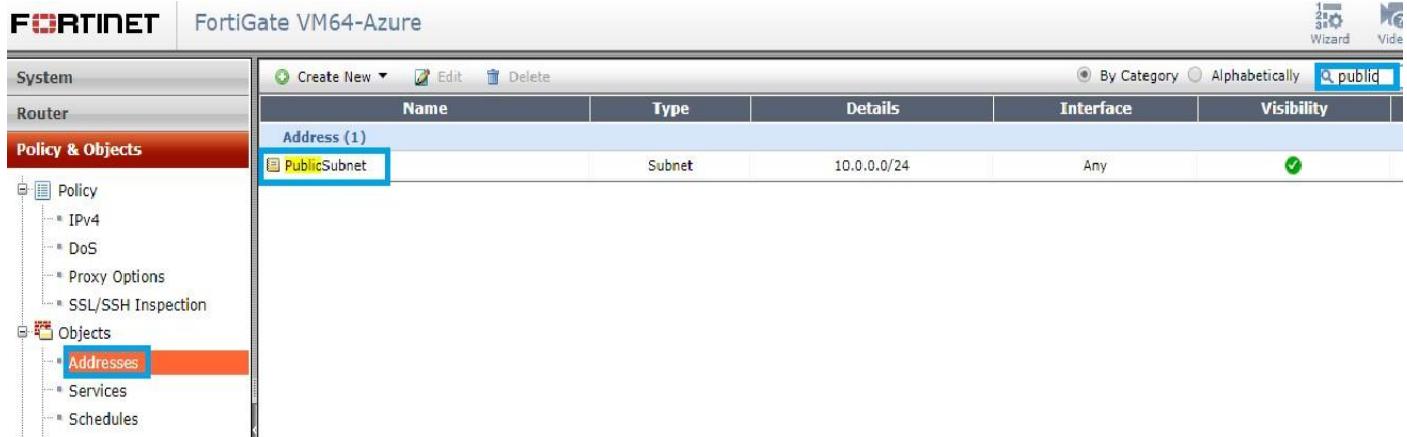
fortigate (PublicSubnet) # set type ipmask

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	<input checked="" type="checkbox"/>

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

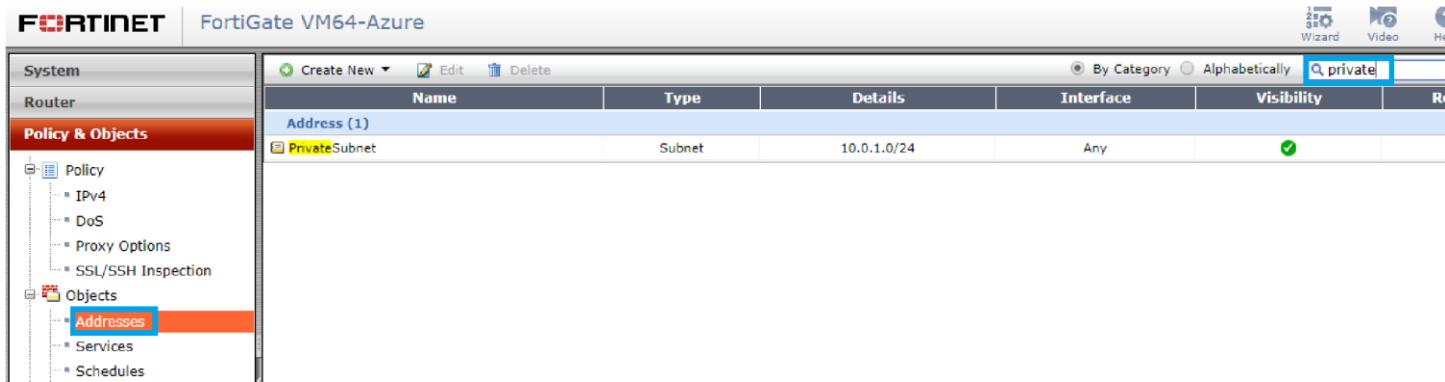
fortigate (PrivateSubnet) # set subnet 10.0.1.0 255.255.255.0

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.



Name	Type	Details	Interface	Visibility
PrivateSubnet	Subnet	10.0.1.0/24	Any	<input checked="" type="checkbox"/>

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

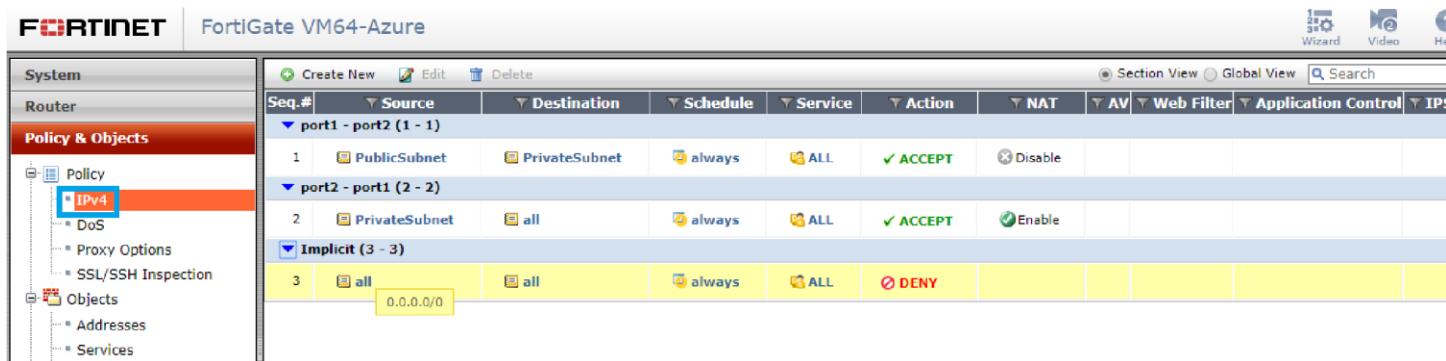
fortigate (3) # set action accept

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.



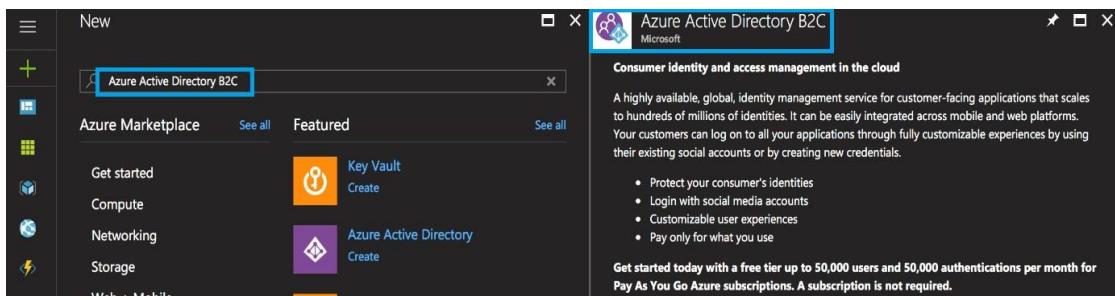
Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IP
1	PublicSubnet	PrivateSubnet	always	ALL	✓ ACCEPT	Disable				
2	PrivateSubnet	all	always	ALL	✓ ACCEPT	Enable				
3	all	all	always	ALL	✗ DENY					

4.2. Azure B2C Tenant Creation and Configuration

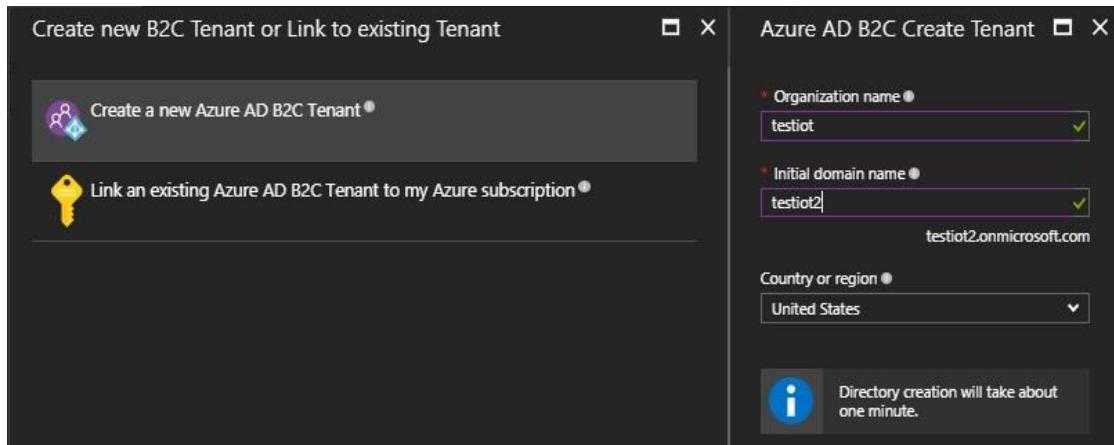
Creating Azure AD B2C tenant is a one-time activity, if you have a B2C Tenant already created by your admin then you should be added into that tenant as Global Administrator to register your app to get the B2C tenant id, application id and sign-in/sign-up policies.

Follow Below steps to create Azure AD B2C Tenant:

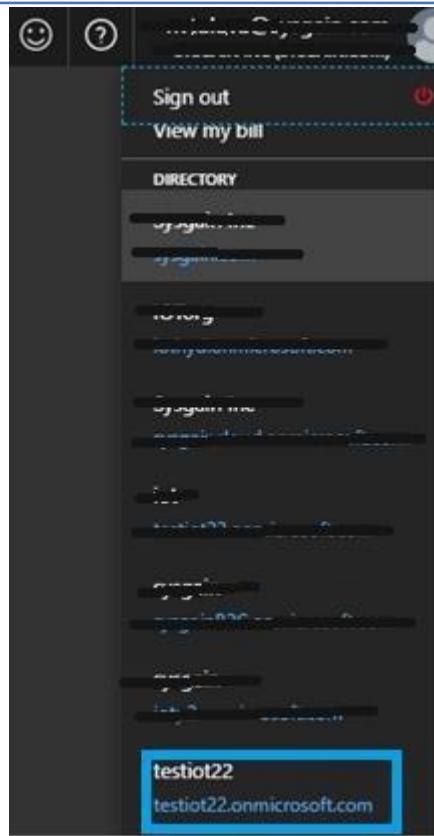
1. Create a new B2C tenant in **Azure Active Directory B2C**. You'll be shown a page with the information on Azure Active Directory B2C. Click **Create** at the bottom to start configuring your new Azure Active Directory B2C tenant.



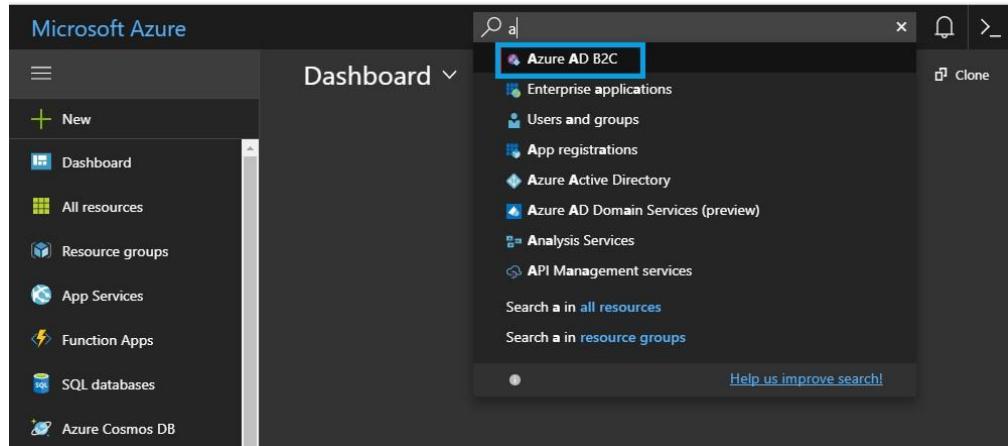
2. Choose the **Organization name**, **Initial Domain name** and **Country or Region** for your Tenant.



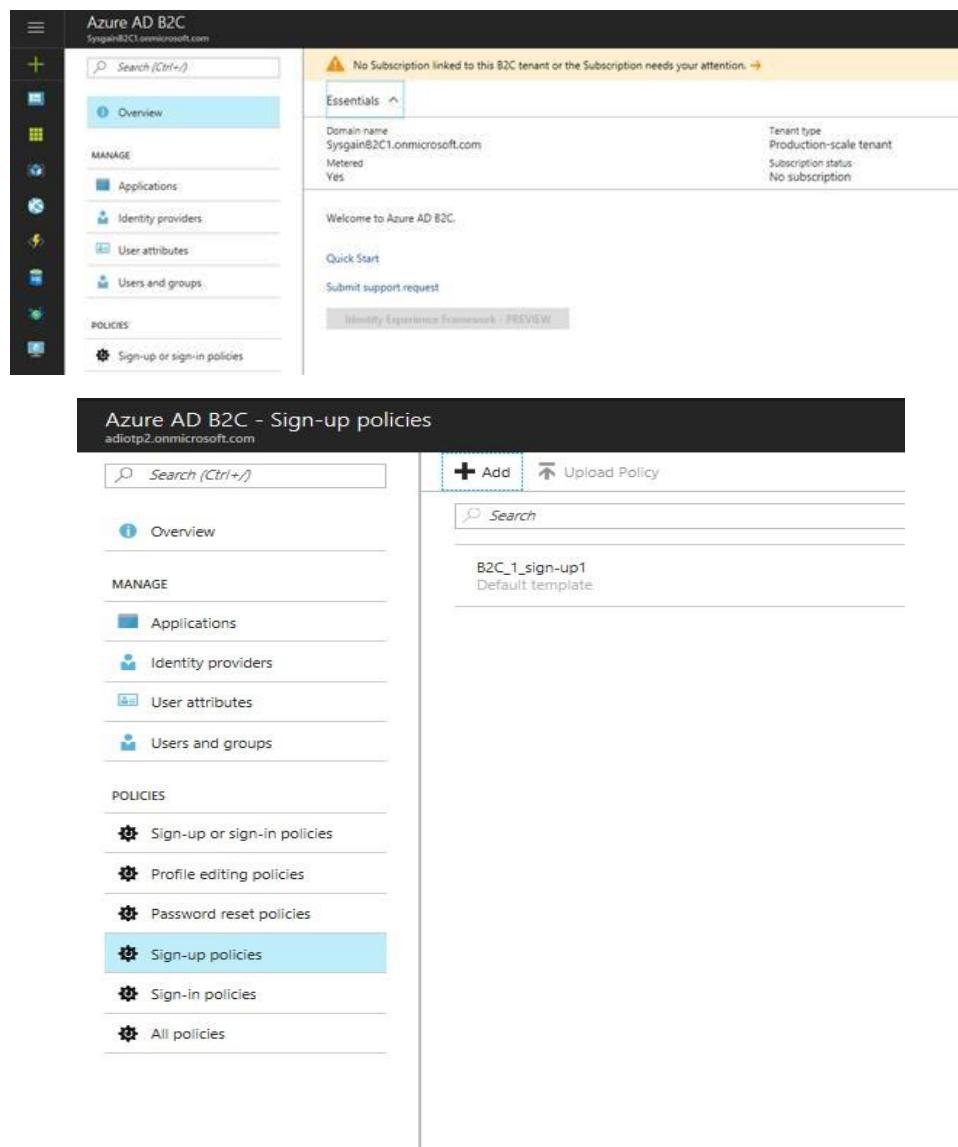
3. Once the B2C Tenant is created, you will see the below confirmation under the portal login user name.



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 two side-by-side Azure AD B2C management interfaces.

Left Panel (Azure AD B2C Overview):

- Header: Azure AD B2C, SysgainB2C1.onmicrosoft.com
- Search bar: Search (Ctrl+)
- Overview button (highlighted in blue)
- Manage section: Applications, Identity providers, User attributes, Users and groups
- Policies section: Sign-up or sign-in policies (highlighted in blue)

Right Panel (Azure AD B2C - Sign-up policies):

- Header: Azure AD B2C - Sign-up policies, adiotp2.onmicrosoft.com
- Search bar: Search (Ctrl+)
- Add button (+) and Upload Policy button
- Search bar: Search
- List of policies:
 - 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 <small>i</small>	<input type="text" value="sign-up1"/> ✓
* Identity providers <small>i</small>	<input type="checkbox"/> Email signup > 1 Selected
Sign-up attributes <small>i</small>	<input type="checkbox"/> 0 Selected >
Application claims <small>i</small>	<input type="checkbox"/> 0 Selected >
Multifactor authentication <small>i</small>	<input type="checkbox"/> Off >
Page UI customization <small>i</small>	<input type="checkbox"/> Default >

Create **OK**

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

Add policy X

New sign-up policy

* Name <small>i</small>	<input type="text" value="sign-up1"/> ✓
* Identity providers <small>i</small>	<input type="checkbox"/> Email signup > 1 Selected
Sign-up attributes <small>i</small>	<input type="checkbox"/> 0 Selected >
Application claims <small>i</small>	<input type="checkbox"/> 0 Selected >
Multifactor authentication <small>i</small>	<input type="checkbox"/> Off >
Page UI customization <small>i</small>	<input type="checkbox"/> Default >

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

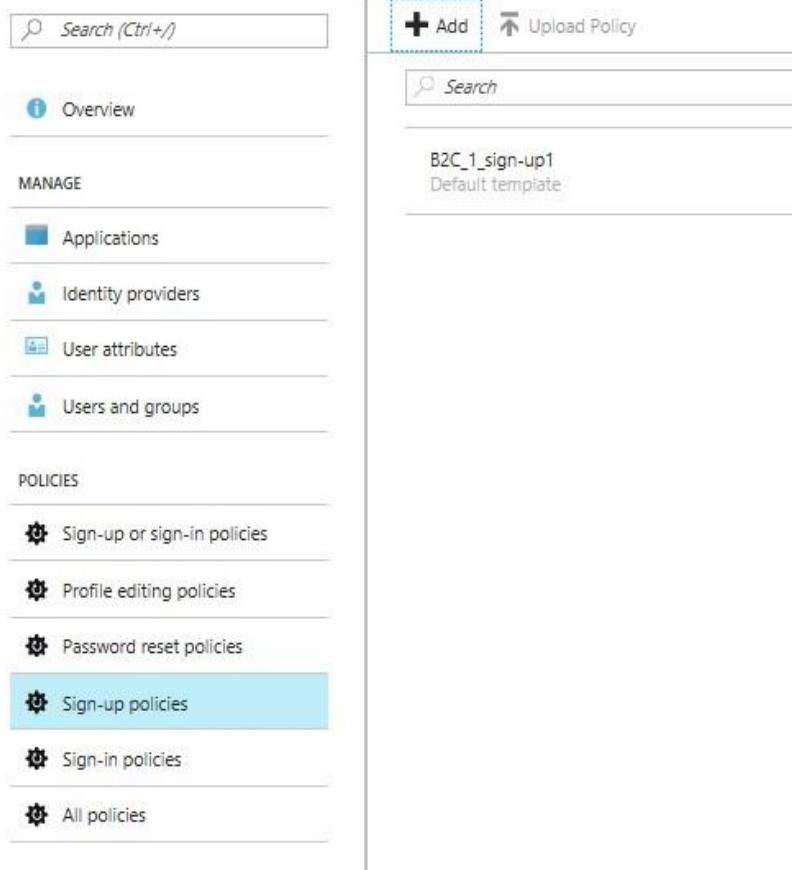
Application claims ⓘ >
13 Selected

Multifactor authentication ⓘ >
Off

Page UI customization ⓘ >
Default

Create

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

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

The screenshot shows the Azure AD B2C Sign-up policies page. On the left, there's a sidebar with 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' option is highlighted with a blue background. At the top right, there are 'Add' and 'Upload Policy' buttons, and a search bar.

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** (highlighted)
- Sign-in policies
- All policies

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

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

Search (Ctrl+ /)

+ Add Upload Policy

Search

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
- Sign-up policies
- Sign-in policies (highlighted)
- All policies

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

Add policy □ X

New sign-in policy

* Name sign-in1

* Identity providers 0 Selected

Application claims 0 Selected

Multifactor authentication Off

Page UI customization Default

Create

Select identity providers □ X

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

OK

11. Select all Application claim

Add policy

New sign-in policy

* Name sign-in1

* Identity providers 1 Selected

Application claims 0 Selected

Multifactor authentication Off

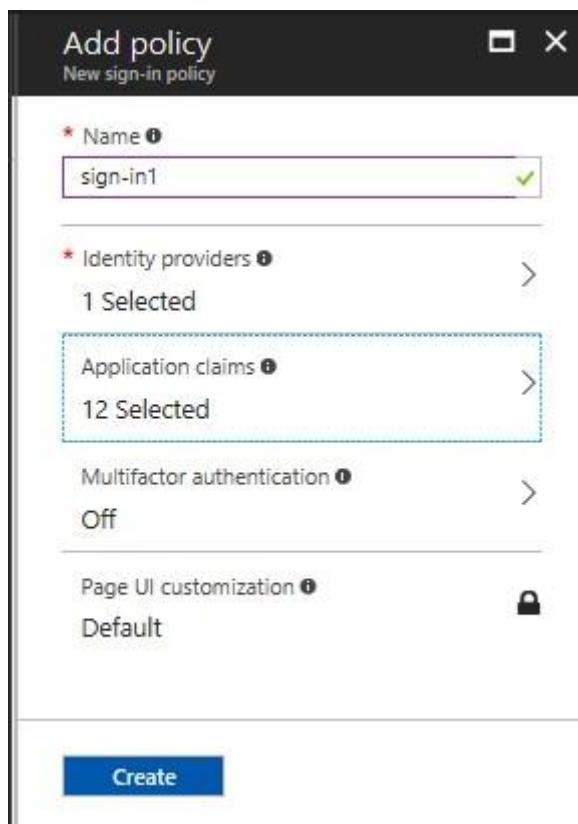
Page UI customization Default

Select application claims

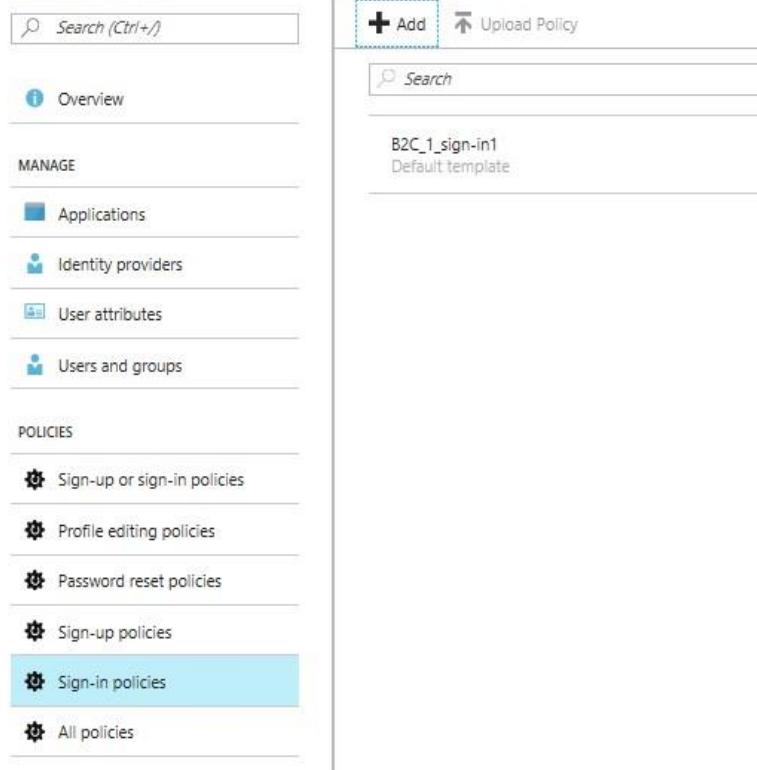
NAME	CLAIM TYPE	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	city	String	The city in which the user is located.	Built-in
Country/Region	country	String	The country/region in which the user is located.	Built-in
Display Name	displayName	String	Display Name of the User	Built-in
Email Addresses	emailis	StringCollection	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

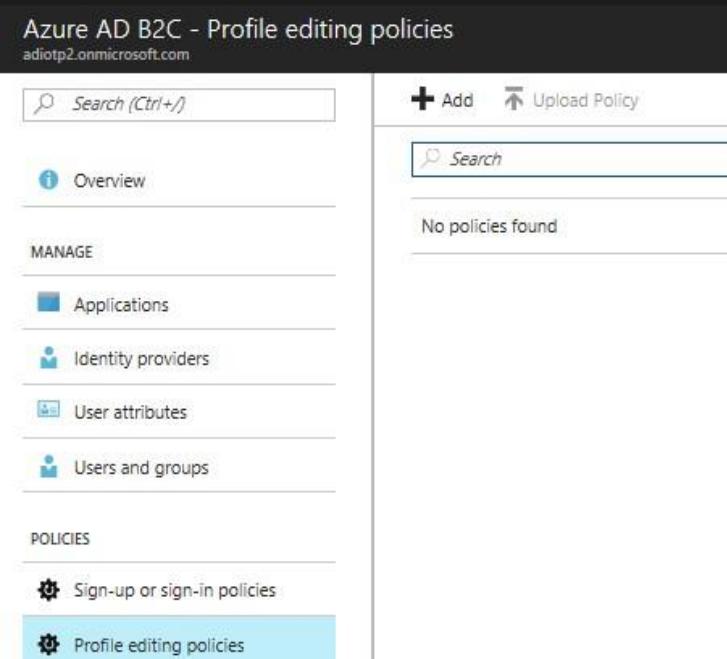
12. Once done, click on **Create**.



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

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

The screenshot shows the Azure AD B2C - Sign-in policies interface. On the left, a sidebar lists 'MANAGE' and 'POLICIES' sections. Under 'POLICIES', 'Sign-in policies' is highlighted with a blue background. At the top right, there are 'Add' and 'Upload Policy' buttons. In the main area, a search bar is at the top, followed by a list item: 'B2C_1_sign-in1 Default template'.

14. Click on **Profile editing policies**

The screenshot shows the Azure AD B2C - Profile editing policies interface. The sidebar is identical to the previous screenshot. Under 'POLICIES', 'Profile editing policies' is highlighted with a blue background. At the top right, there are 'Add' and 'Upload Policy' buttons. In the main area, a search bar is at the top, followed by a message: 'No policies found'.

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

Add policy
 New profile editing policy

*	Name <small>?</small>
	profile-edit1 ✓
*	Identity providers <small>?</small>
	0 Selected >
	Profile attributes <small>?</small>
	0 Selected >
	Application claims <small>?</small>
	0 Selected >
	Page UI customization <small>?</small>
	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 <small>?</small>
	profile-edit1 ✓
*	Identity providers <small>?</small>
	1 Selected >
	Profile attributes <small>?</small>
	0 Selected >
	Application claims <small>?</small>
	0 Selected >
	Page UI customization <small>?</small>
	Default 🔒

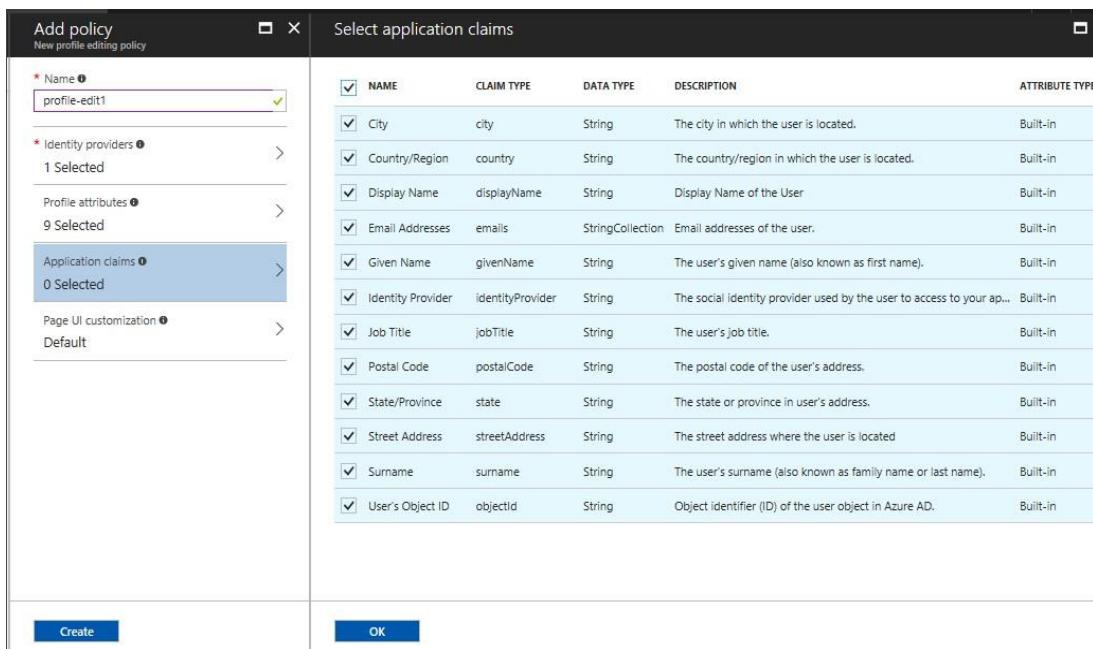
Create

Select profile attributes

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"/> 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

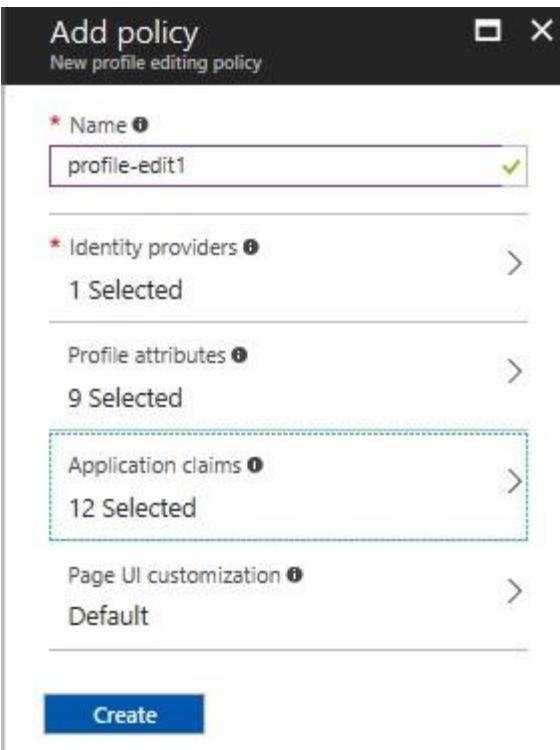
OK

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

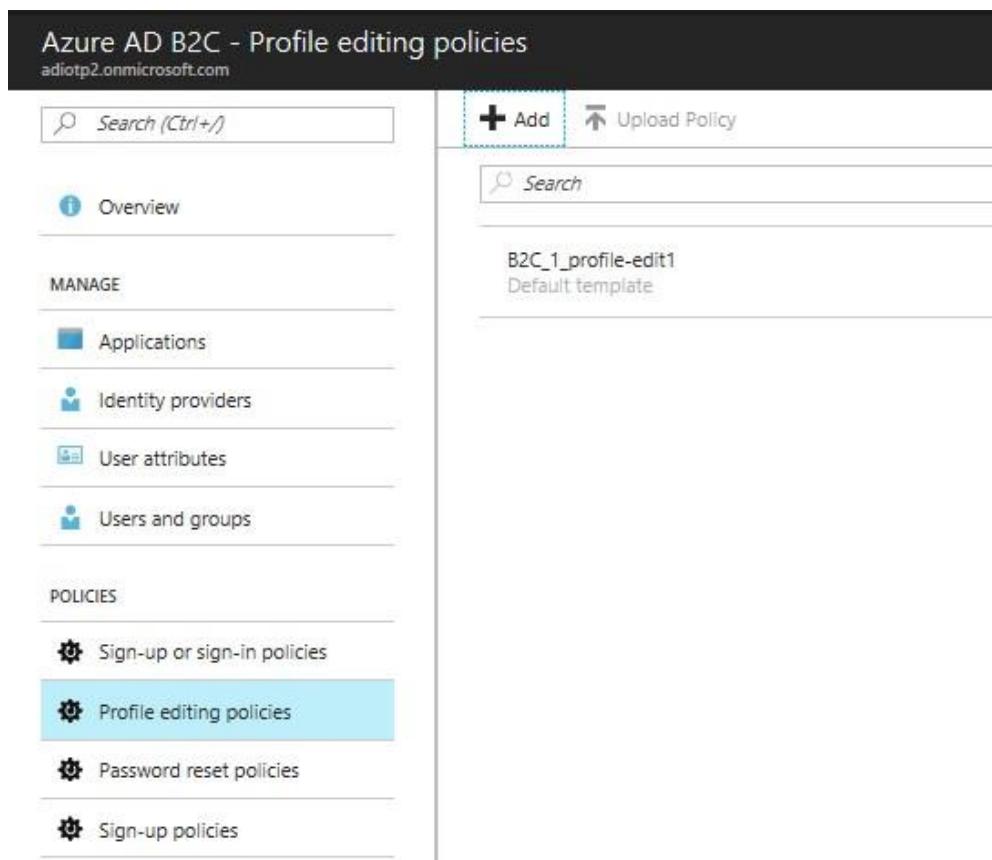


NAME	CLAIM TYPE	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	city	String	The city in which the user is located.	Built-in
Country/Region	country	String	The country/region in which the user is located.	Built-in
Display Name	displayName	String	Display Name of the User	Built-in
Email Addresses	emails	StringCollection	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

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



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



The screenshot shows the Azure AD B2C - Profile editing 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). The 'Profile editing policies' option is highlighted with a blue background. The main right area shows a list of policies with a search bar at the top. One policy is listed: 'B2C_1_profile-edit1' (Default template).

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

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

Search (Ctrl+Shift+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
New password reset policy

* Name **password-change1**

* Identity providers **0 Selected**

Application claims **0 Selected**

Multifactor authentication **Off**

Page UI customization **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

Create

Select identity providers

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

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

Create

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

OK

24. Click on **Create**.

Add policy X

New password reset policy

* Name !
password-change1 ✓

* Identity providers ! >
1 Selected

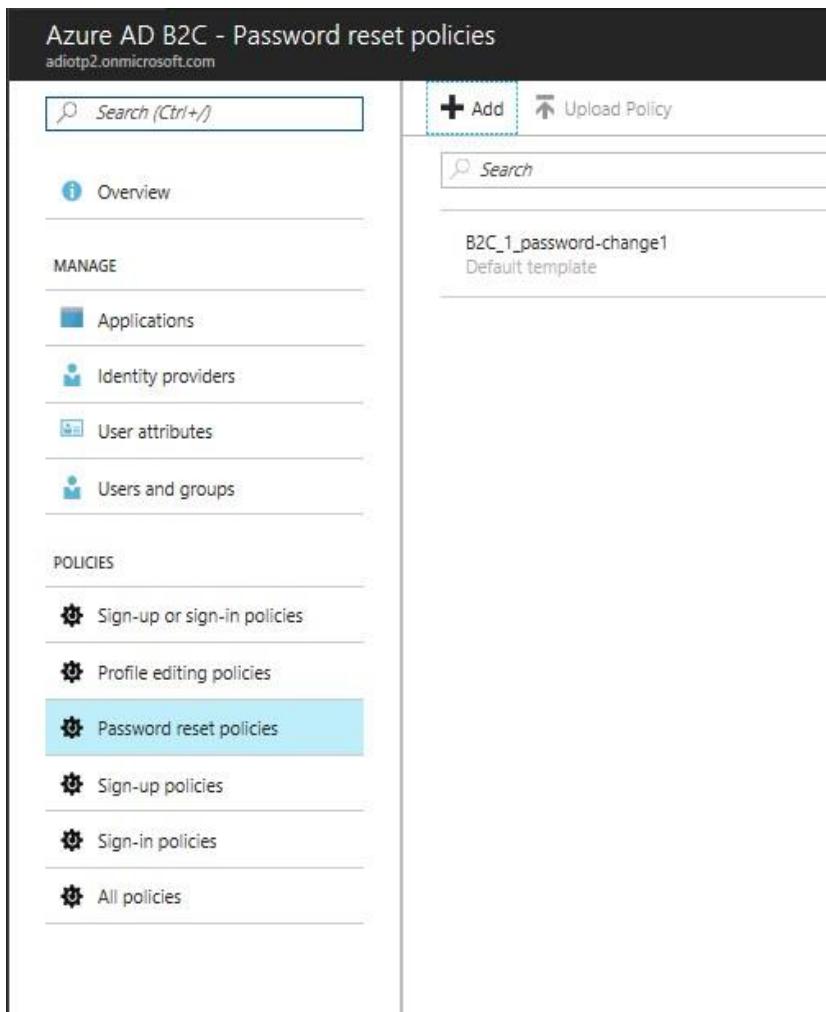
Application claims ! >
11 Selected

Multifactor authentication ! >
Off

Page UI customization ! >
Default

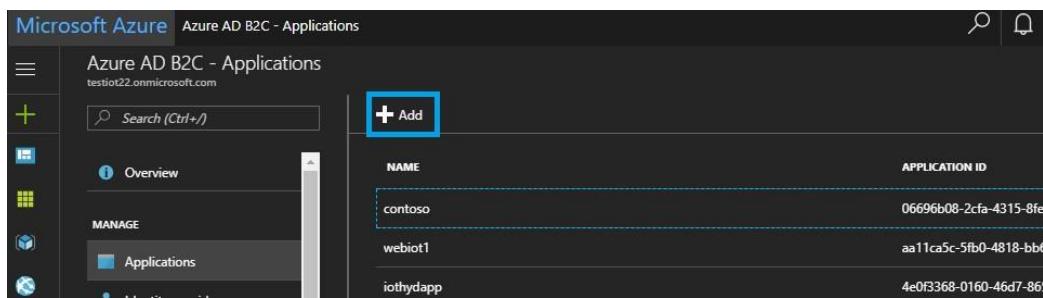
Create

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



The screenshot shows the Azure AD B2C - Password reset policies interface. The left sidebar has a search bar and navigation links for Overview, Applications, Identity providers, User attributes, and Users and groups under the MANAGE section. Under POLICIES, the 'Password reset policies' link is highlighted with a blue background. The main content area shows a single policy named 'B2C_1_password-change1' with the status 'Default template'. There are 'Add' and 'Upload Policy' buttons at the top of the main content area.

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 - Applications interface. The left sidebar has a search bar and navigation links for Overview, Applications, and more under the MANAGE section. The 'Applications' link is highlighted. The main content area shows a table of applications with columns for NAME and APPLICATION ID. Three applications are listed: 'contoso' (Application ID: 06696b08-2cfa-4315-8fe), 'webiot1' (Application ID: aa11ca5c-5fb0-4818-bb6), and 'iothydapp' (Application ID: 4e0f3368-0160-46d7-865). A large blue '+' Add button is located at the top right of the table.

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

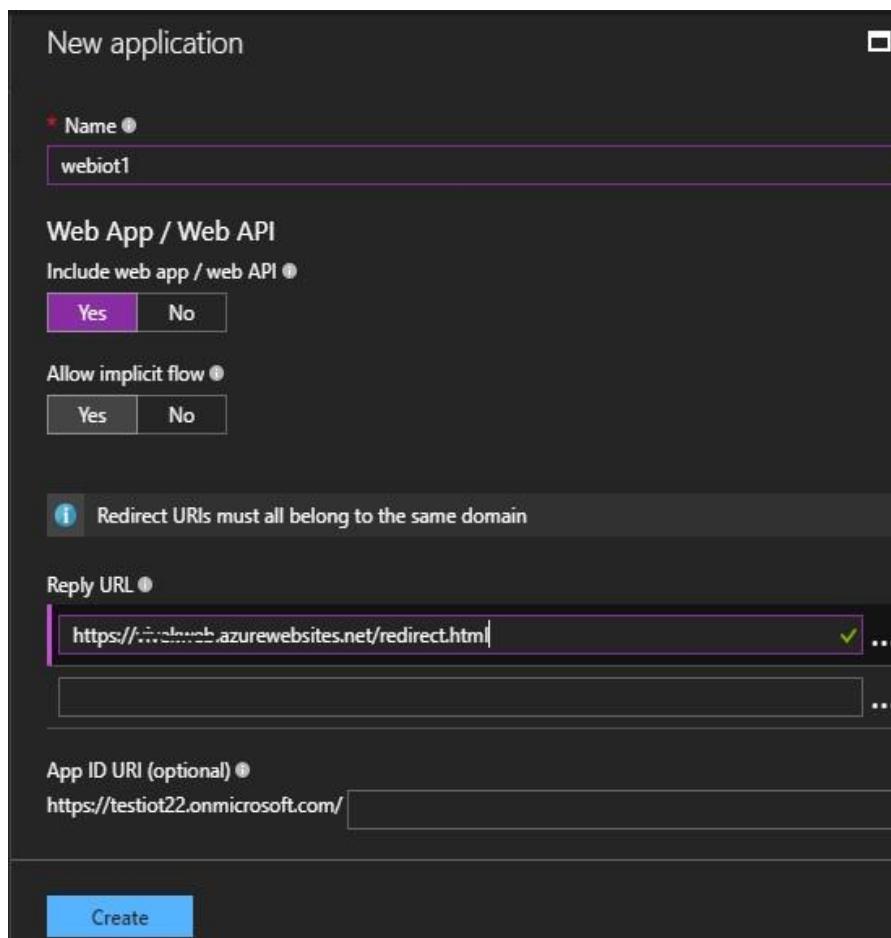
`https://<name of the web app>.azurewebsites.net/redirect.html`

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

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

After that, click on **Create**.

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



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

Azure AD B2C - Applications
testiot22.onmicrosoft.com

NAME	APPLICATION ID
contoso	06696b08-2cfa-4315-85
webiot1	aa11ca5c-5fb0-4818-bb
iothyapp	4e0f3368-0160-46d7-8
demoapp	991b1d9c-5504-4a8e-a

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

webiot1 - Keys

GENERAL
Properties
Keys

Save Discard **Generate key**

App key ●
26X*****

30. **Copy** the secret key.

webiot1 - Keys

GENERAL
Properties
Keys

Save Discard **Generate key**

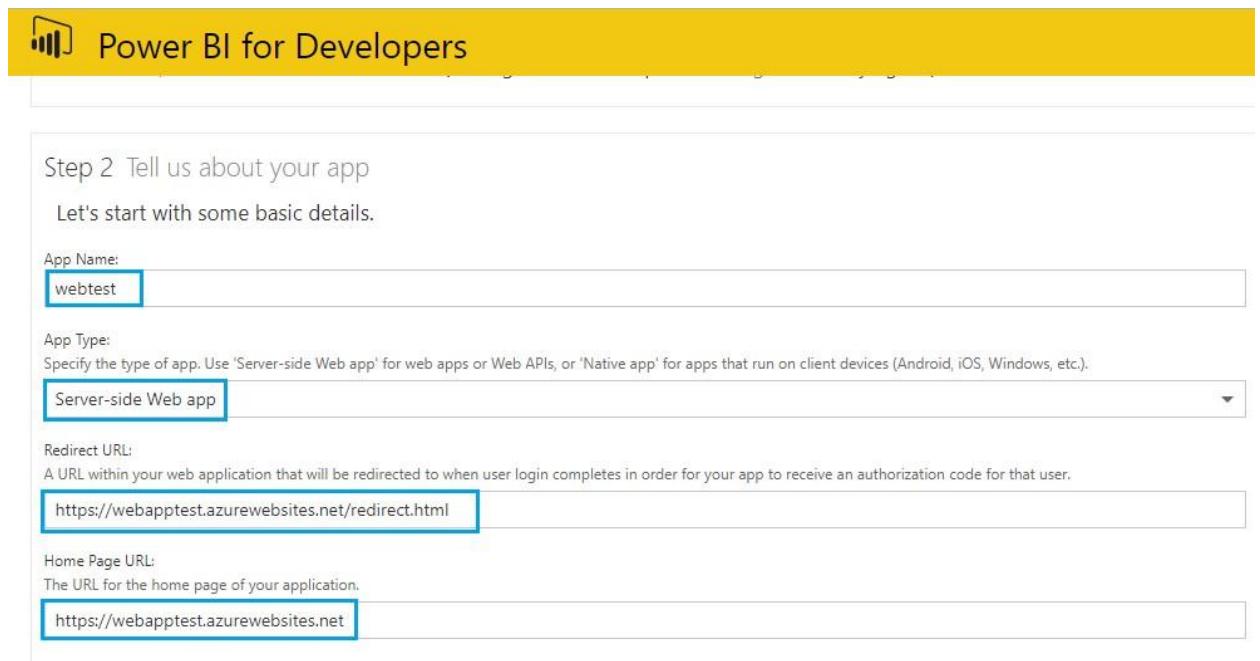
App key ●
26X*****
%\$88MxGK"\$vr6Ofz

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.



Power BI for Developers

Step 2 Tell us about your app

Let's start with some basic details.

App Name: webtest

App Type: Server-side Web app

Redirect URL: https://webapptest.azurewebsites.net/redirect.html

Home Page URL: 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/BMdBimml2xDkrbnvoqw+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

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

Overview Quick start 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

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

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

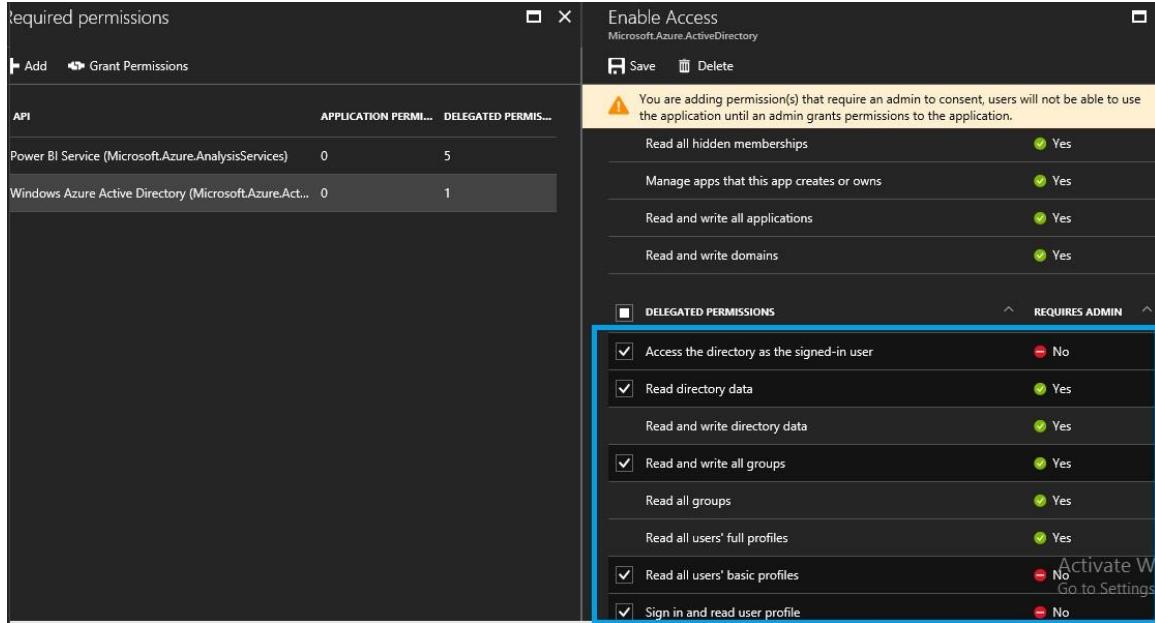
TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

- 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 windows from the Azure portal.

Required permissions:

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

Enable Access (Microsoft.Azure.ActiveDirectory):

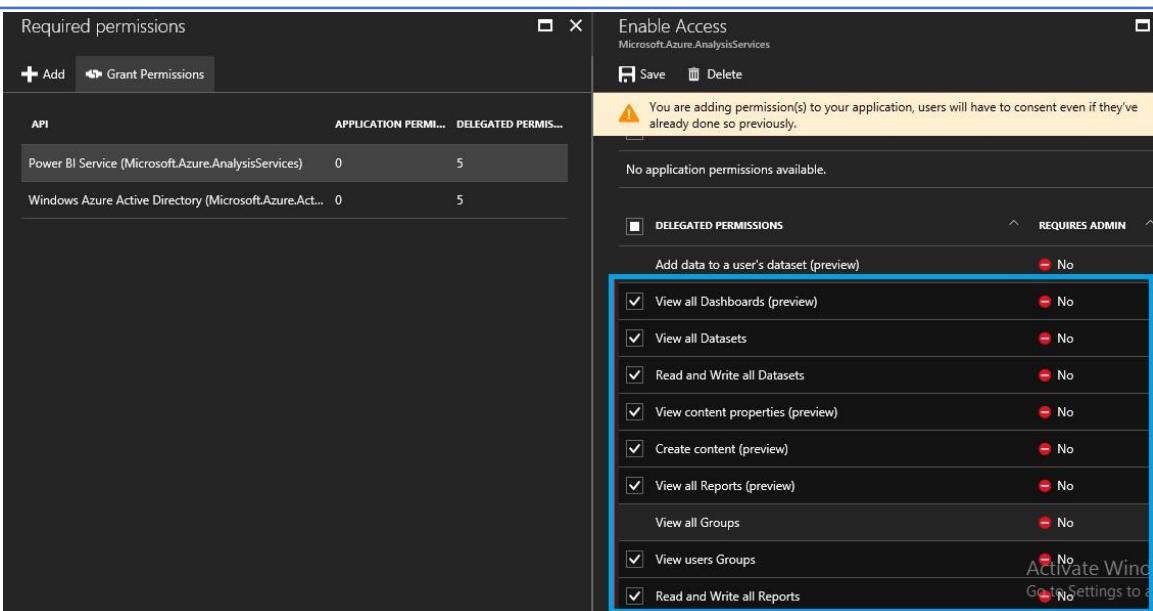
You are adding permission(s) that require an admin to consent; users will not be able to use the application until an admin grants permissions to the application.

DELEGATED PERMISSIONS

- Access the directory as the signed-in user No
- Read directory data Yes
- Read and write directory data Yes
- Read and write all groups Yes
- Read all groups Yes
- Read all users' full profiles No
- Read all users' basic profiles No
- 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



The screenshot shows two adjacent windows from the Azure portal.

Left Window: Required permissions

- Header: API, APPLICATION PERMIS..., DELEGATED PERMIS...
- Table:

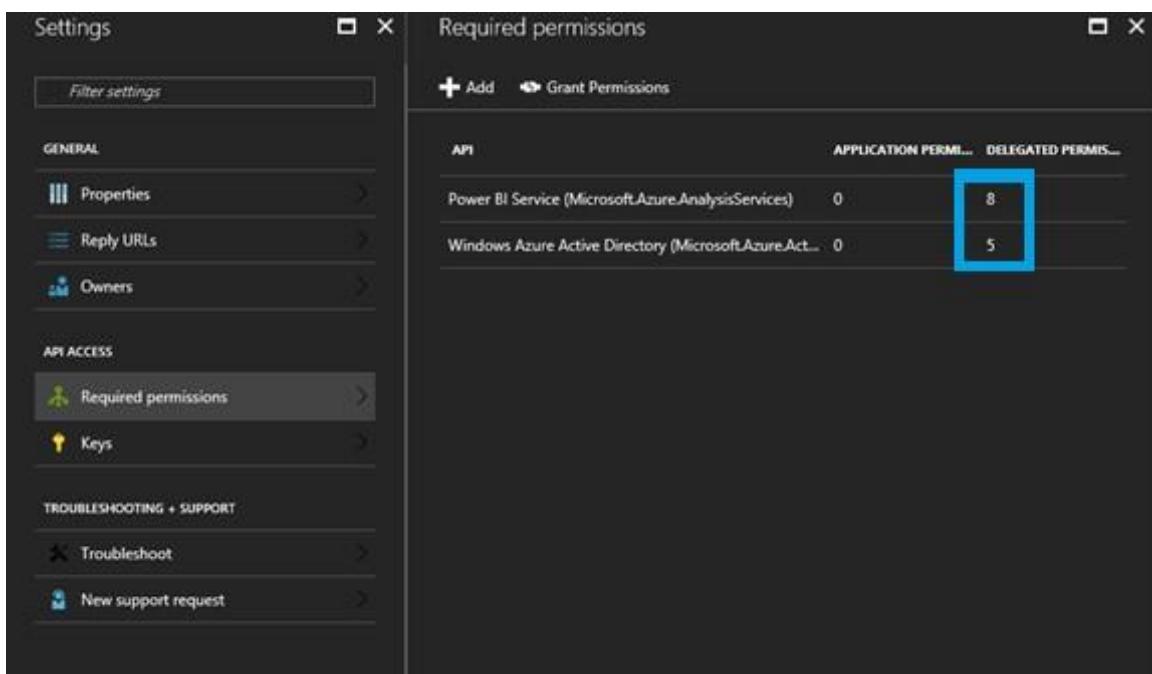
API	APPLICATION PERMIS...	DELEGATED PERMIS...
Power BI Service (Microsoft.Azure.AnalysisServices)	0	5
Windows Azure Active Directory (Microsoft.Azure.Act...	0	5

Right Window: Enable Access

- Header: Microsoft.Azure.AnalysisServices
- Buttons: Save, Delete
- Warning message: You are adding permission(s) to your application, users will have to consent even if they've already done so previously.
- Text: No application permissions available.
- Section: DELEGATED PERMISSIONS (Requires Admin)

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

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



The screenshot shows two windows side-by-side.

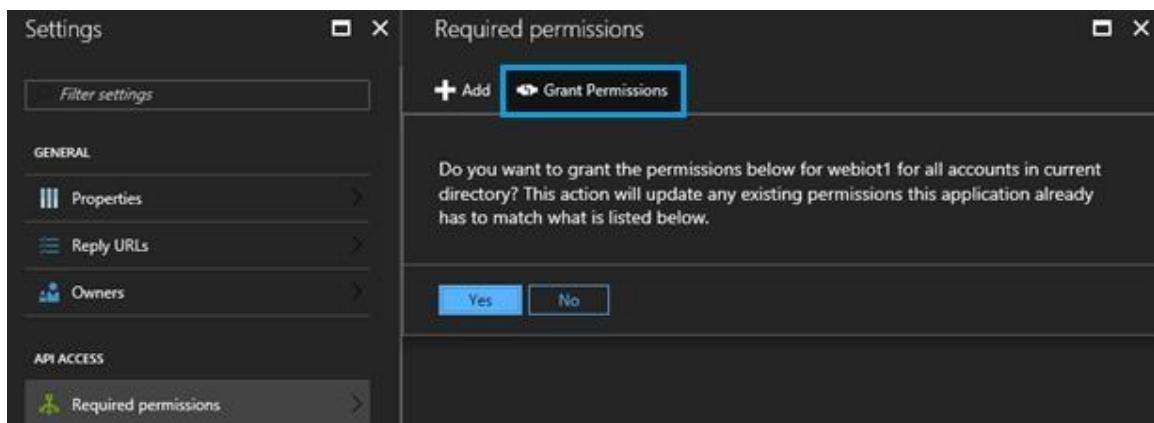
Left Window: Settings

- Header: Filter settings
- GENERAL
 - Properties
 - Reply URLs
 - Owners
- API ACCESS
 - Required permissions (selected)
 - Keys
- TROUBLESHOOTING + SUPPORT
 - Troubleshoot
 - New support request

Right Window: Required permissions

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

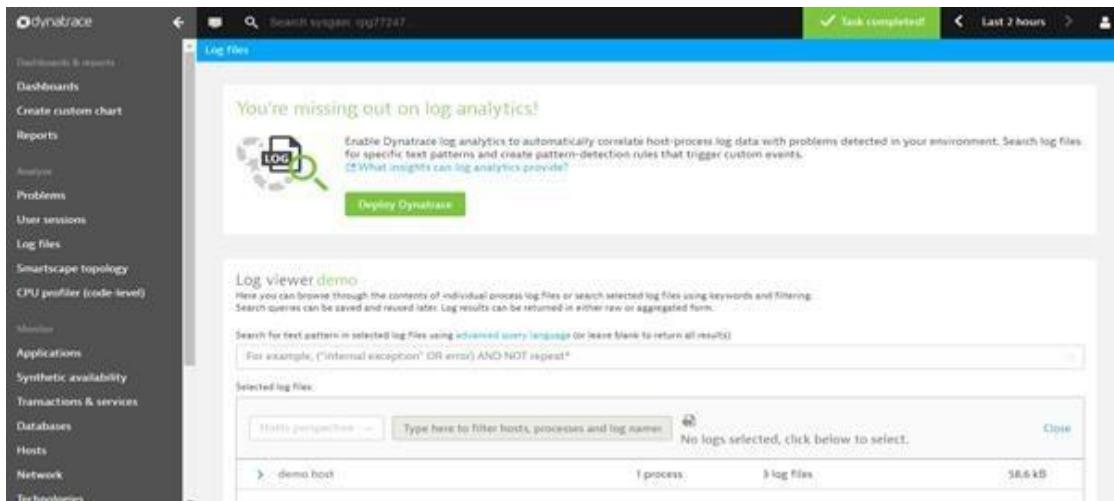
7. Click on **Grant Permissions**, then click **Yes**.



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”**.

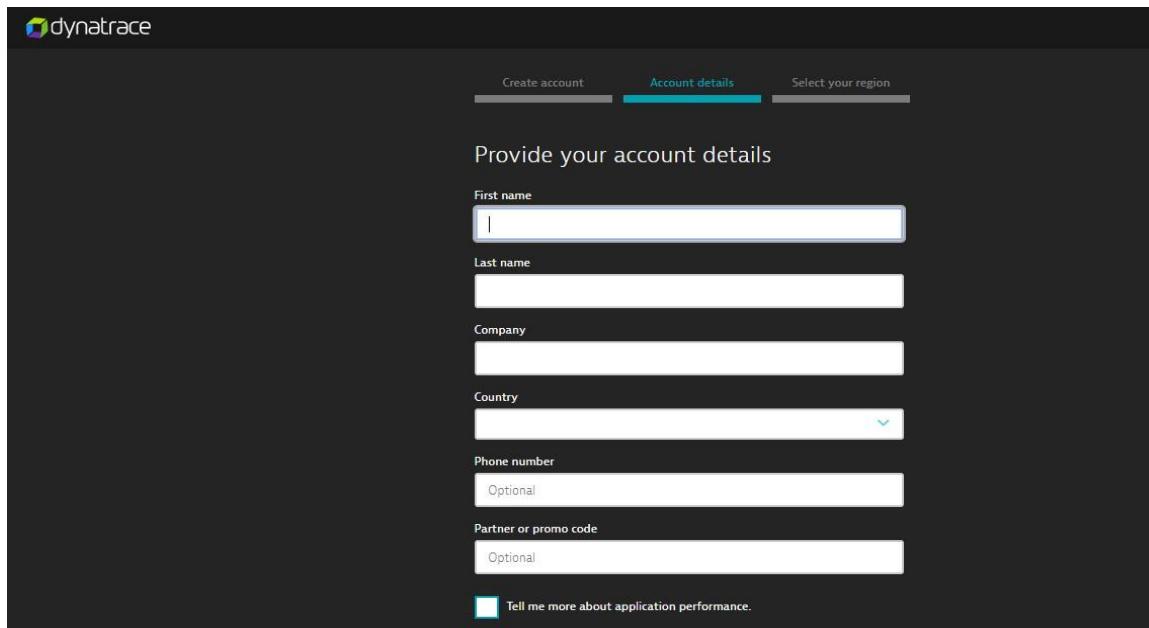
Dynatrace home page - <https://www.dynatrace.com>



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

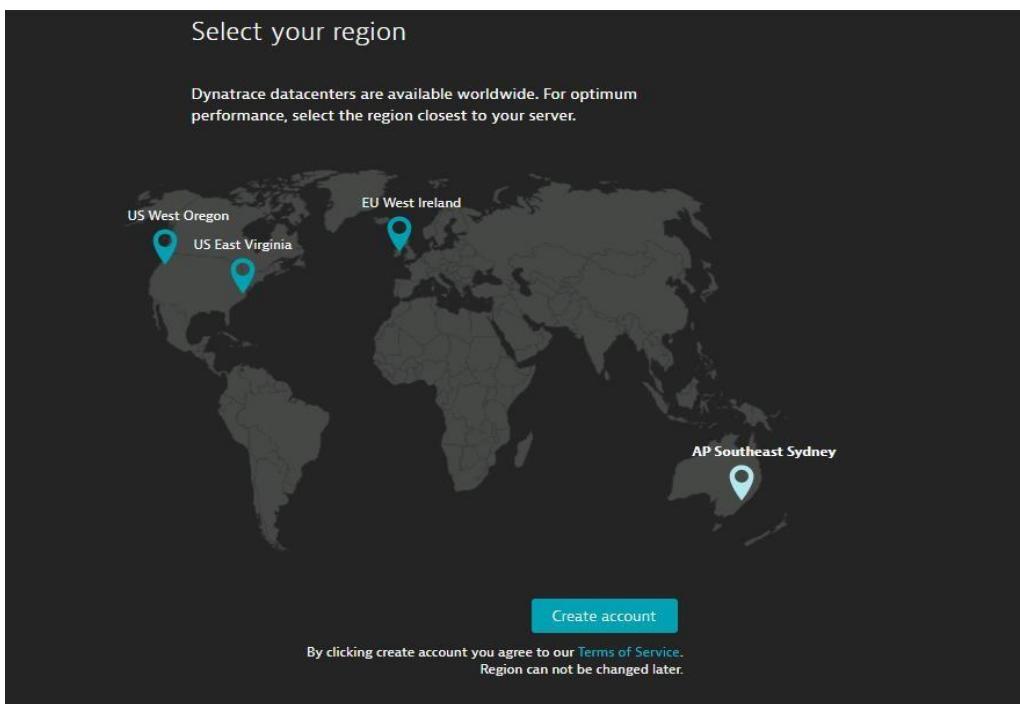


2. The below screen will appear. Fill out the **Create account**, **Account details** and **Select your region** screens.

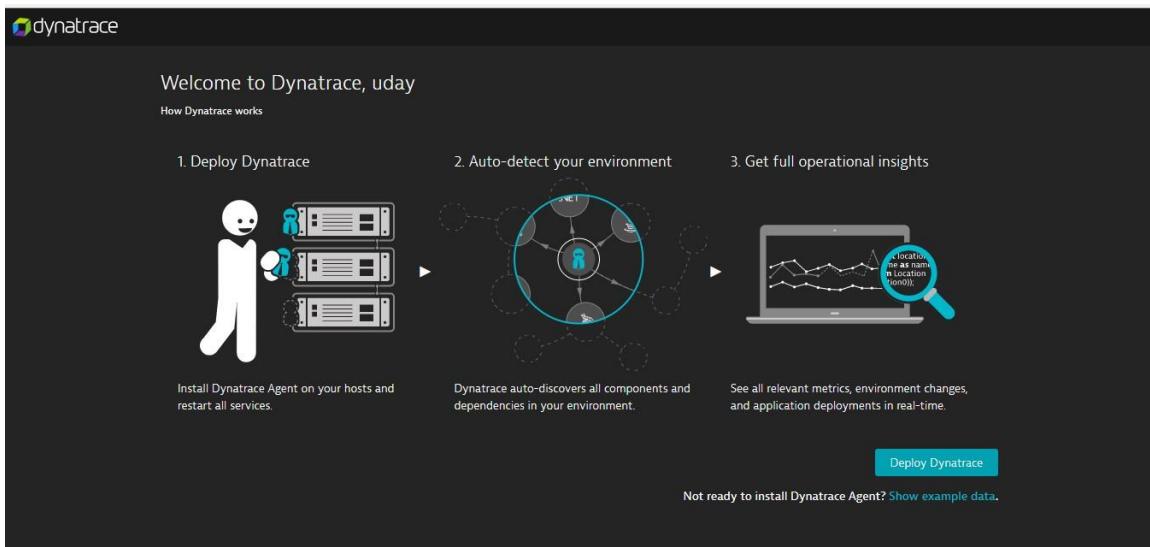


The screenshot shows the 'Account details' step of the Dynatrace sign-up process. The form includes fields for First name, Last name, Company, Country, Phone number, and Partner or promo code, all marked as optional. A checkbox at the bottom allows users to tell more about application performance.

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



4. Click on “**Deploy Dynatrace**”.



5. Click on “**Start installation**”.

Dynatrace

Search sysgain: rpg77247...

Start here

Deploy Dynatrace

Deploy Dynatrace

Monitor all your real users and technologies by installing OneAgent

A single Dynatrace OneAgent monitors real user experience and all the technologies, services, and applications that run in your environment. Just install the agent. No configuration required. [More...](#)



[Start installation](#)

Left sidebar menu:

- Dashboards & reports
- Dashboards
- Create custom chart
- Reports
- Analyze
- Problems
- User sessions
- Log files
- Smartscape topology
- CPU profiler (code-level)
- Monitor
- Applications
- Synthetic availability
- Transactions & services
- Databases
- Hosts
- Network
- Technologies

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

Dynatrace

Search sysgain: rpg77247...

Start here

Deploy Dynatrace > Install OneAgent

Download Dynatrace OneAgent

Select the platform that your applications run on. By continuing you agree to our [Terms of Service](#).

[Windows](#) [Linux](#) [AIX](#)

You can also monitor your PaaS platform.

[Set up PaaS monitoring](#)

Not ready to install Dynatrace OneAgent?
No problem - we can [email the installation instructions](#) to you and you can download the installer later when you're ready.

Firewall troubles? [Dynatrace OneAgent uses secure socket communication \(HTTPS port 443\). If your network policy doesn't allow this, install Dynatrace Security Gateway.](#)

No web server access? [If you can't install Dynatrace OneAgent on your web server, try agentless real user monitoring.](#)

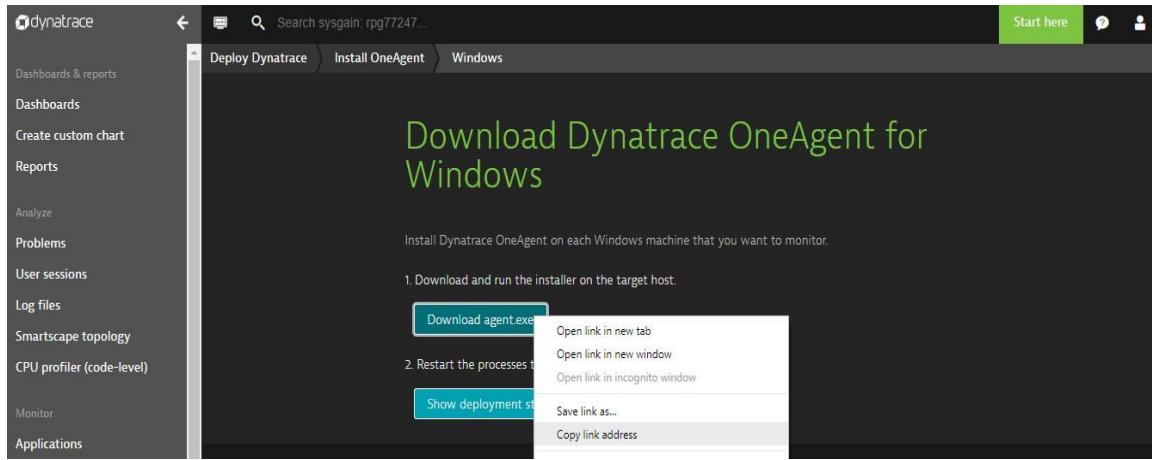
Left sidebar menu:

- Dashboards & reports
- Dashboards
- Create custom chart
- Reports
- Analyze
- Problems
- User sessions
- Log files
- Smartscape topology
- CPU profiler (code-level)
- Monitor
- Applications
- Synthetic availability
- Transactions & services
- Databases
- Hosts
- Network
- Technologies

- 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/enus/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	

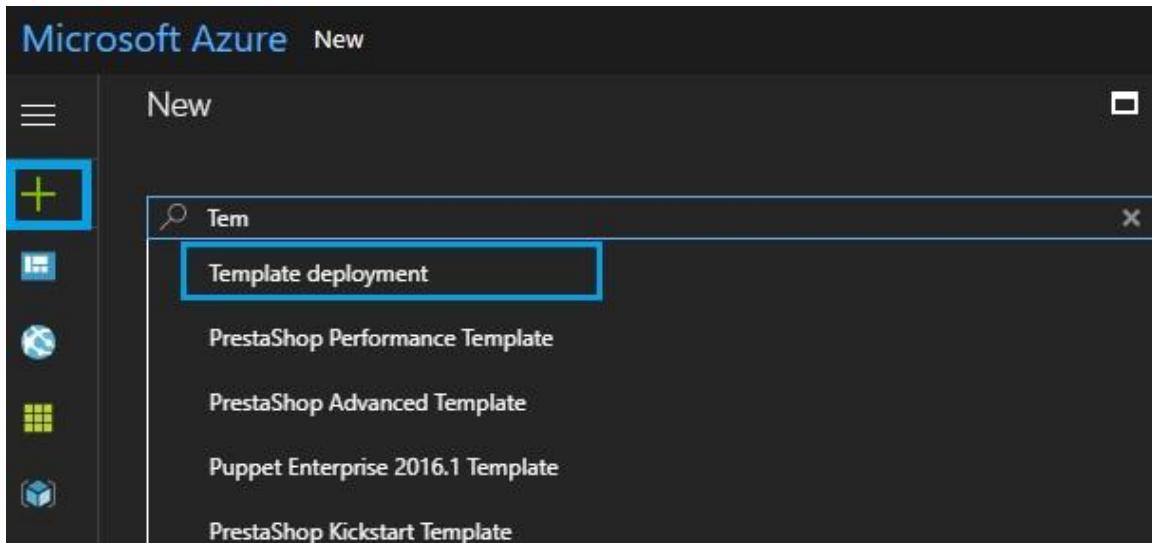
6. Azure Resource Manager Template Deployment

Click on below Git hub repo url <https://github.com/sysgain/iot-automation/tree/sysgainiot>

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

Note: Make sure to deploy [fortigate-main-template.json](#) and [main-template.json](#) in same resource group.

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



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

Microsoft Azure New > Template deployment > Custom 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.

[Create](#)

PUBLISHER Microsoft

LOGICAPP SUPPORTED none

USEFUL LINKS Documentation

Custom deployment Deploy from a custom template

Learn about template deployment

[Read the docs](#)

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

Common templates

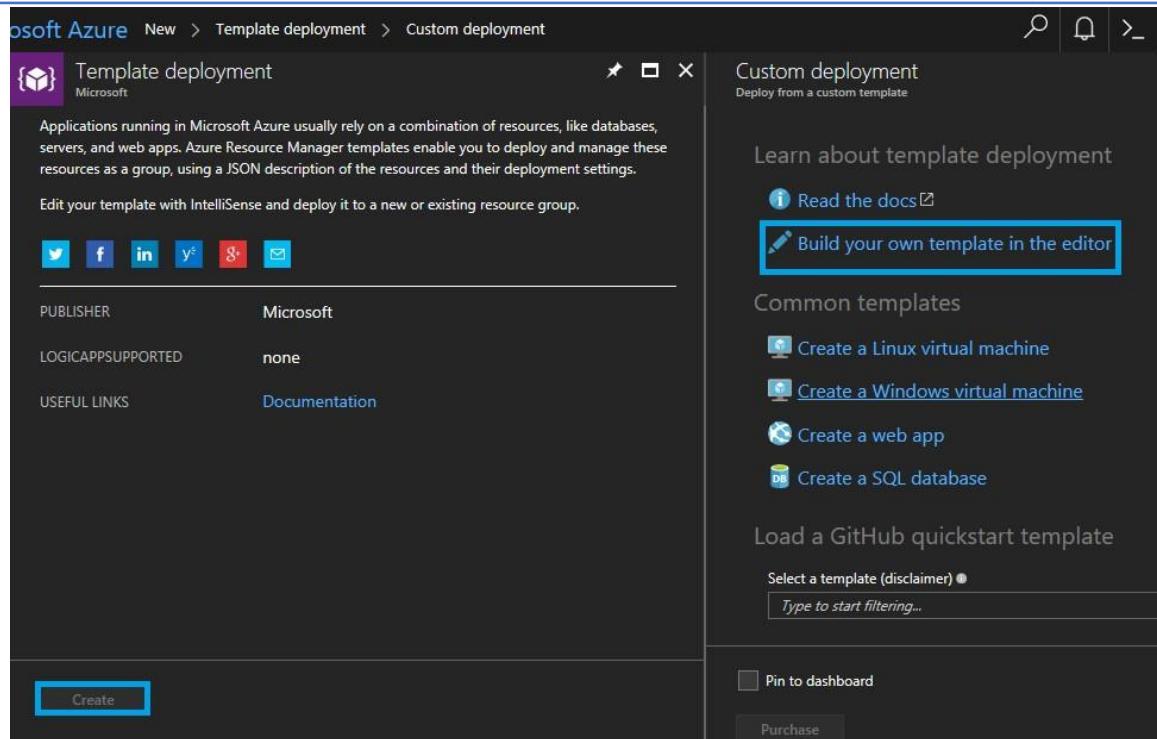
- [Create a Linux virtual machine](#)
- [Create a Windows virtual machine](#)
- [Create a web app](#)
- [Create a SQL database](#)

Load a GitHub quickstart template

Select a template (disclaimer) ● Type to start filtering...

Pin to dashboard

[Purchase](#)



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

Microsoft Azure New > Template deployment > Custom deployment > Edit template

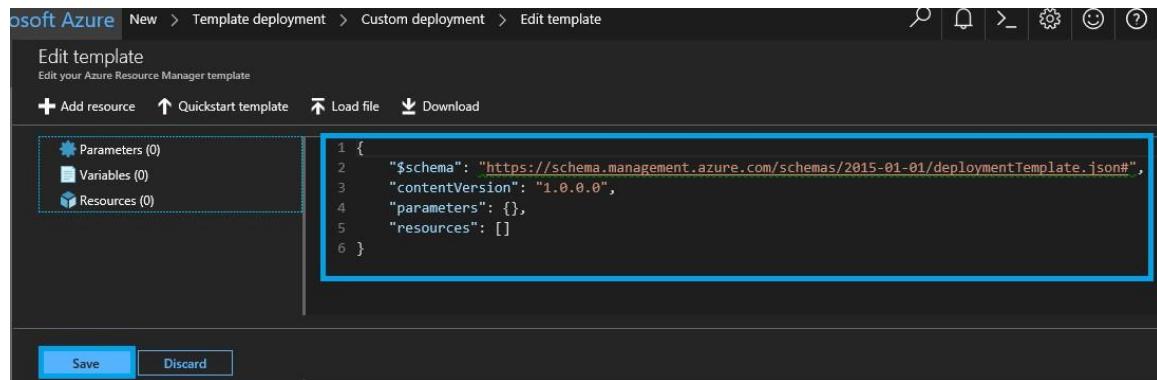
Edit template Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↗ Load file ↘ Download

Parameters (0) Variables (0) Resources (0)

```
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 }
```

[Save](#) [Discard](#)



- 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 ●	user
Chef User Email ●	chefuser@microsoft.com
Chef Org Short Name ●	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

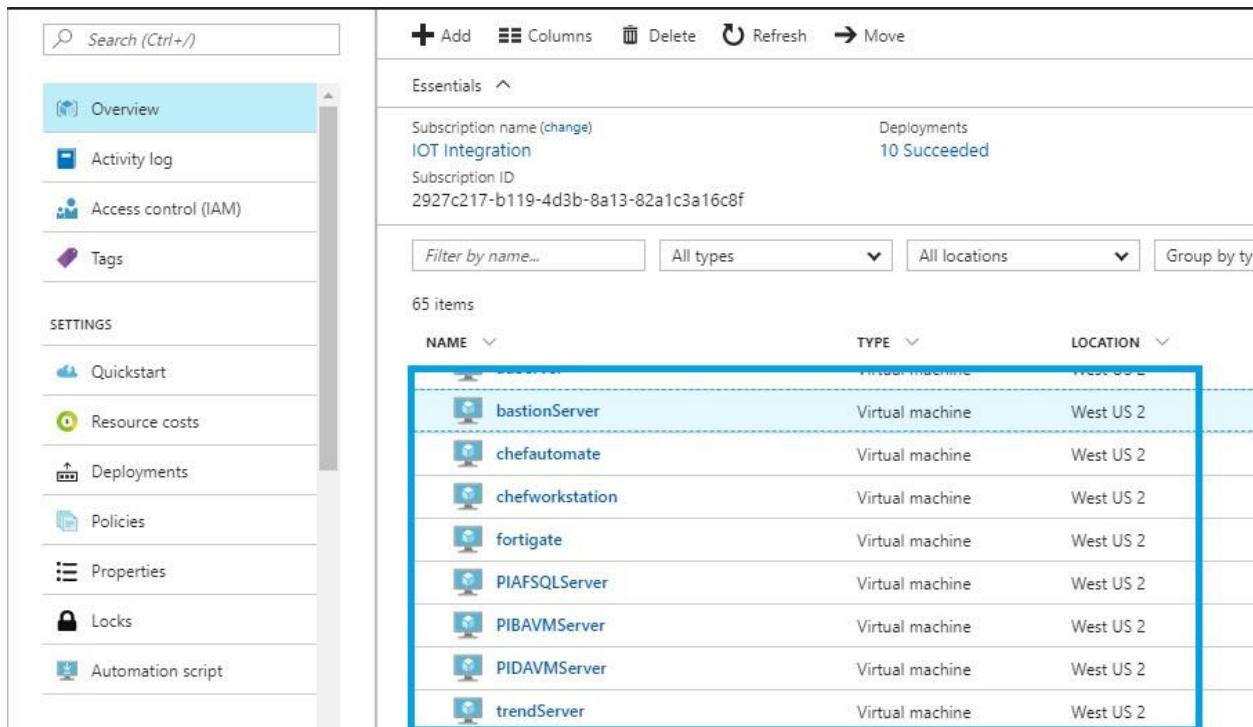
Pin to dashboard

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.



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 wsclientstnh6.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 sqldatabase.windows.net

AZURESQLDBNAME azuredb

AZURESQLUSERNAME sqluser

WINDOWSSQLUSERNAME sqluser

WEBJOBSITEACCNTNAME webjobstrnh6

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.

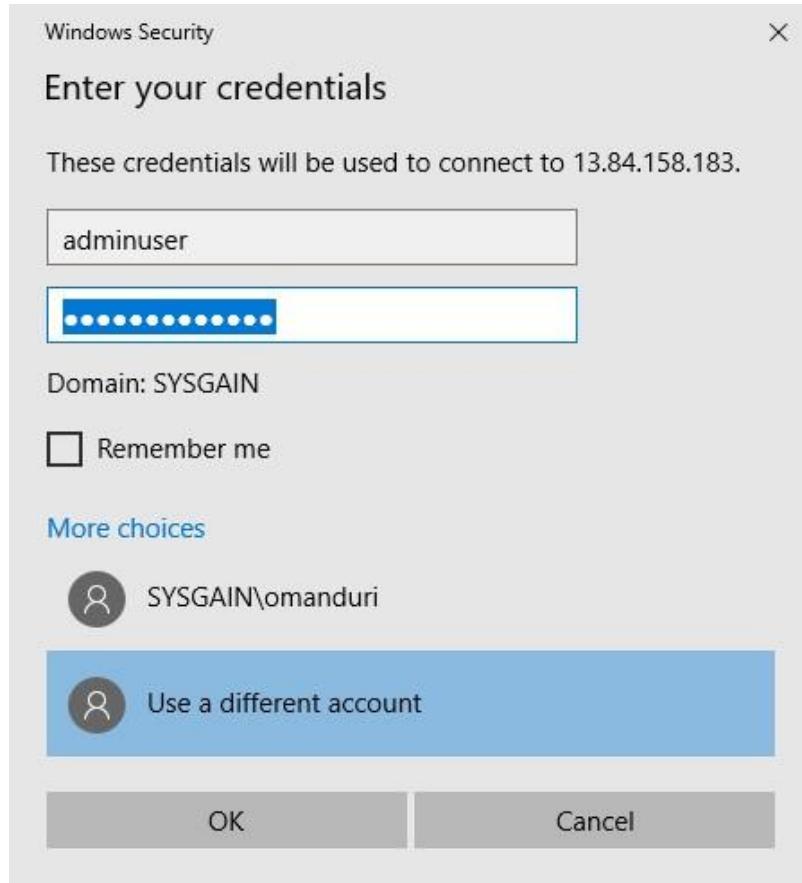
Splunk Enterprise: Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device.

7.1. Dynatrace

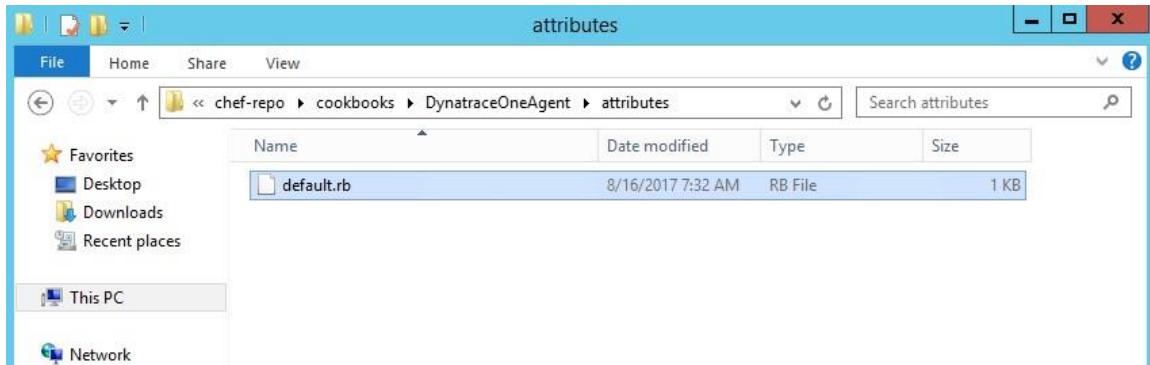
1. Log in to the **Chef Workstation** using the **workstationFQDN** provided in the output section.



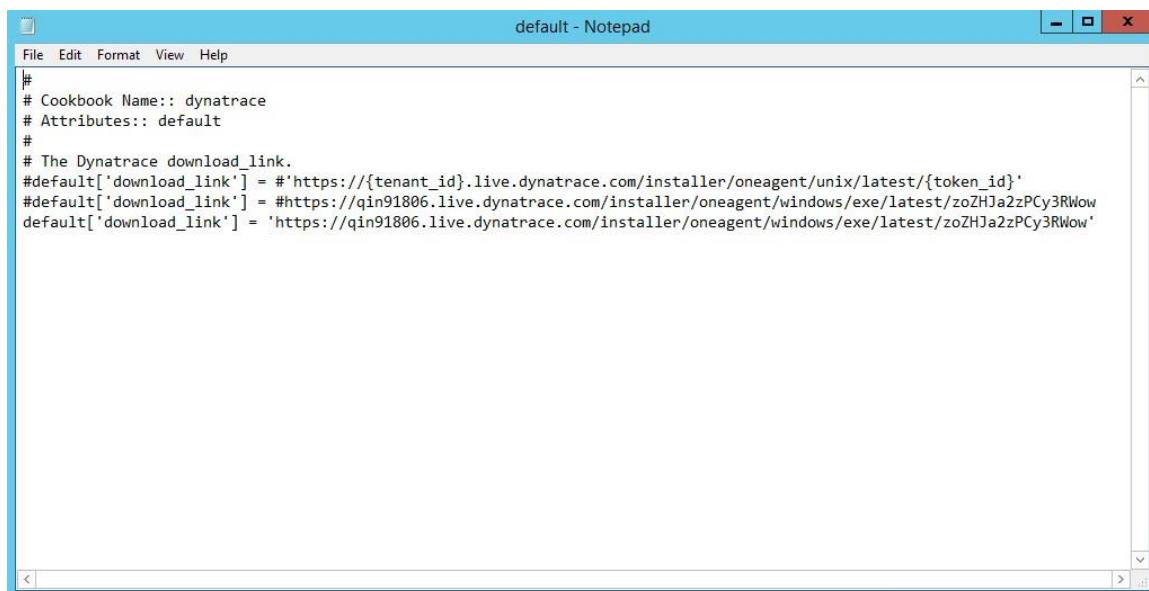
2. Enter the credentials provided in the output section.



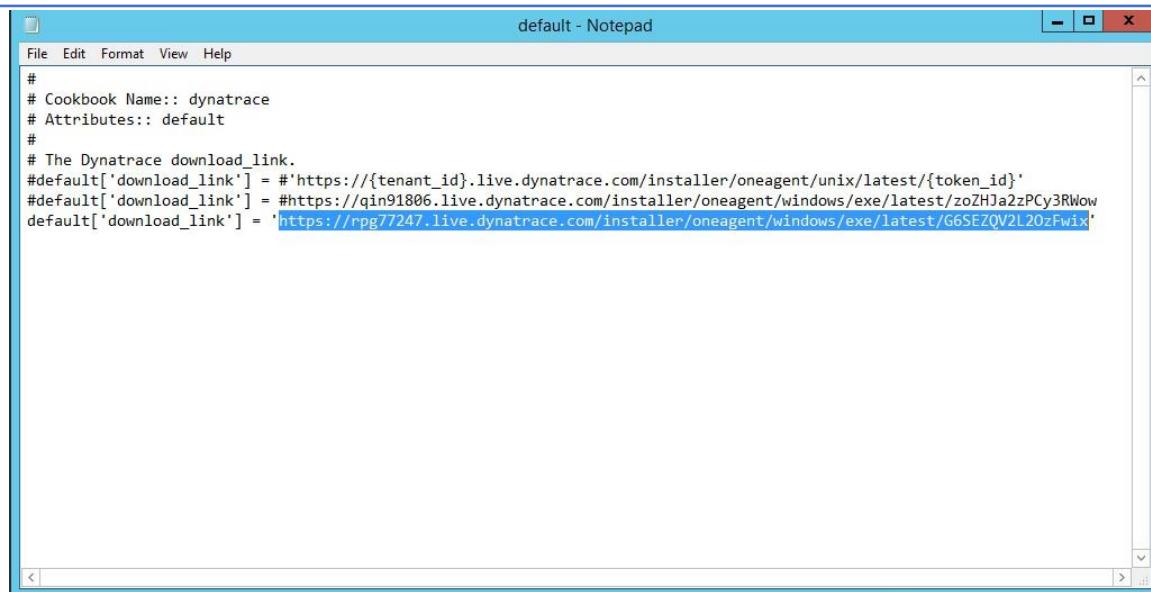
2. After logging in, navigate to **C:\Users\chefrepo\cookbooks\DynatraceOneAgent\attributes** and open the **default.rb** file.



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'
```



A screenshot of a Windows Notepad window titled "default - Notepad". The window contains a block of Chef configuration code:

```
# 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/z0HJa2zPCy3RWo
default['download_link'] = 'https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L20zFwix'
```

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



A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following command being run:

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

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

knife cookbook upload DynatraceOneAgent

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admininuser>cd C:\Users\chef-repo
C:\Users\chef-repo>cd cookbooks\_
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admininuser>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
bastionserverz7yo2.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.

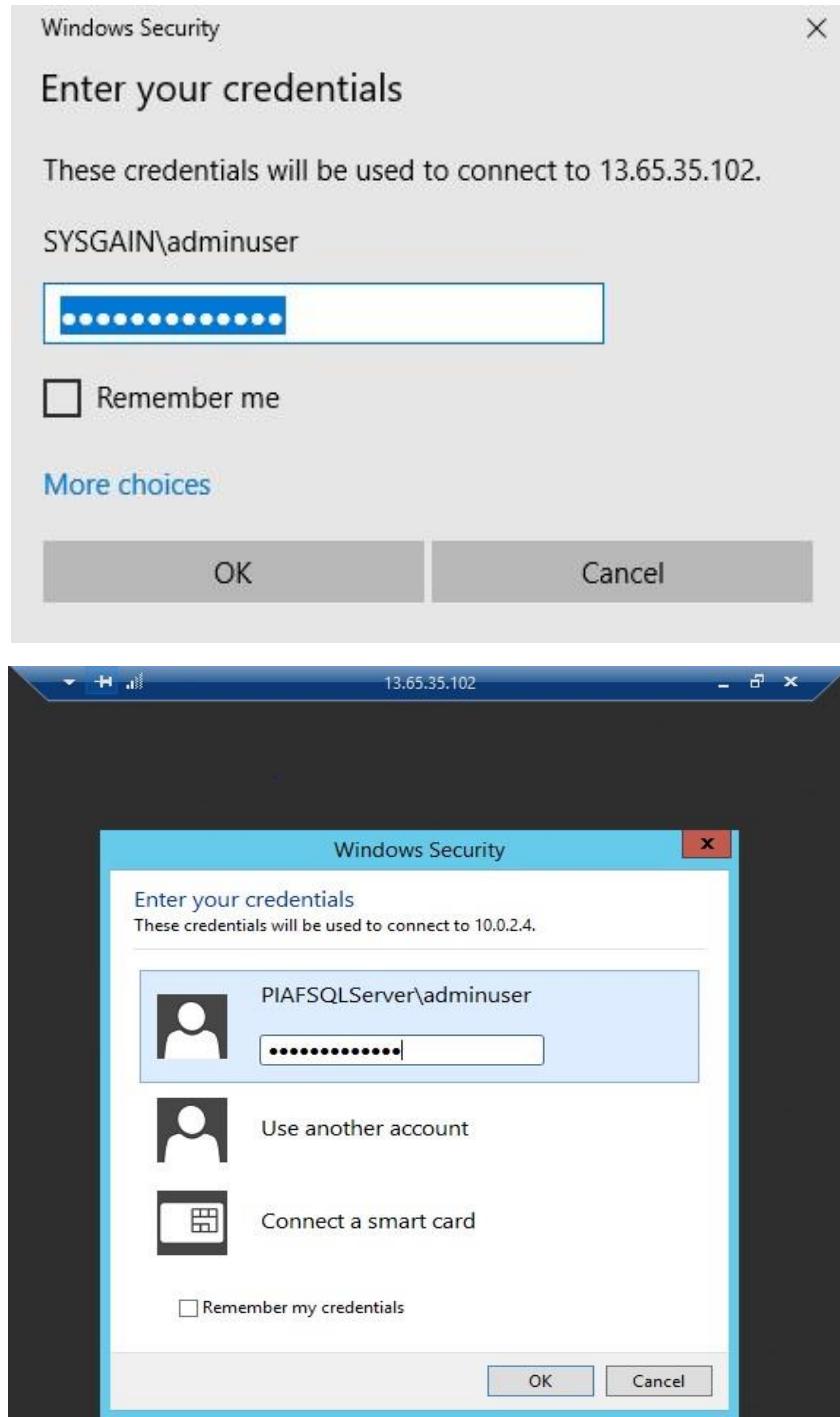
C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserverz7yo2.southcentralus.cloudapp.azure.com
orguser-validator
pidadnsz7yo2.southcentralus.cloudapp.azure.com
wsclientz7yo2.southcentralus.cloudapp.azure.com

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]

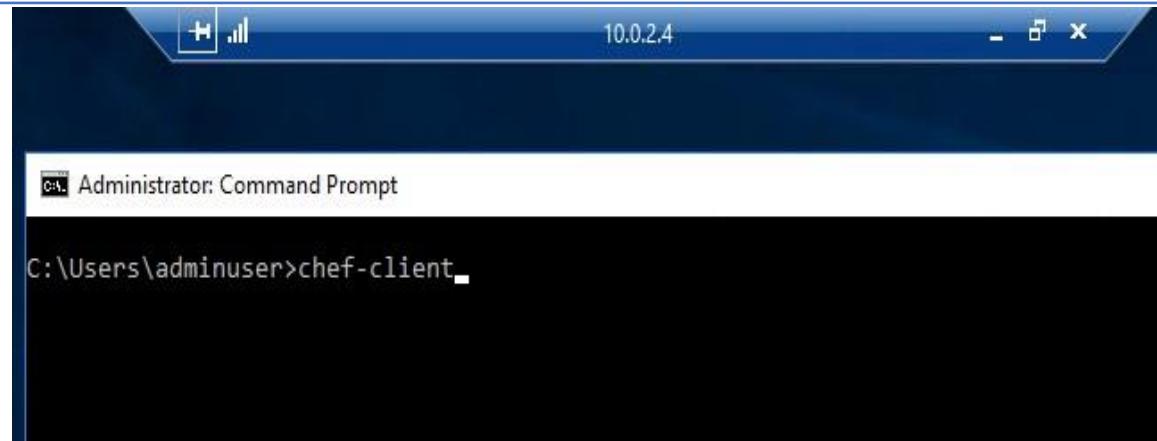
C:\Users\chef-repo\cookbooks>

```

- 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\adminuser>chef-client
```

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

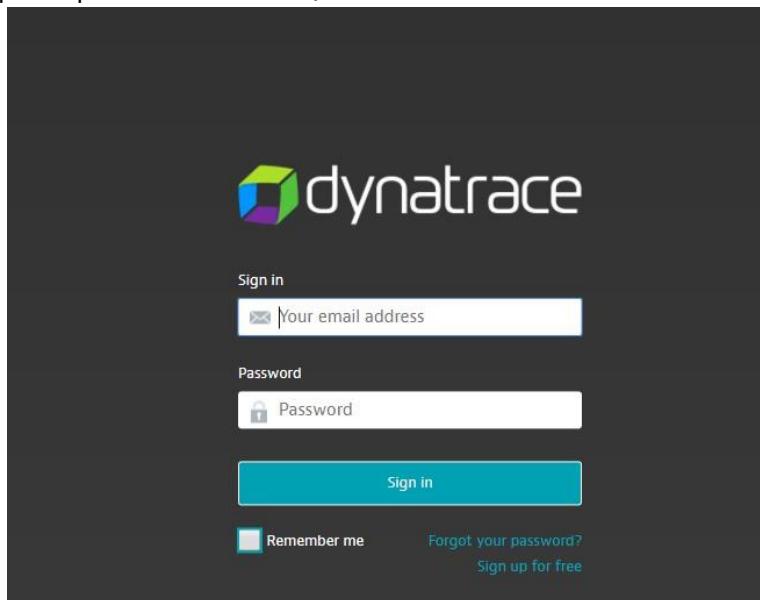
```
- install version latest of package DynatraceOneAgent
* windows_service[Dynatrace OneAgent] action restart[2017-08-16T14:10:56+00:00] INFO: Processing windows_service[Dynatrace OneAgent] action restart (DynatraceOneAgent::oneagent-windows line 28)
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace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

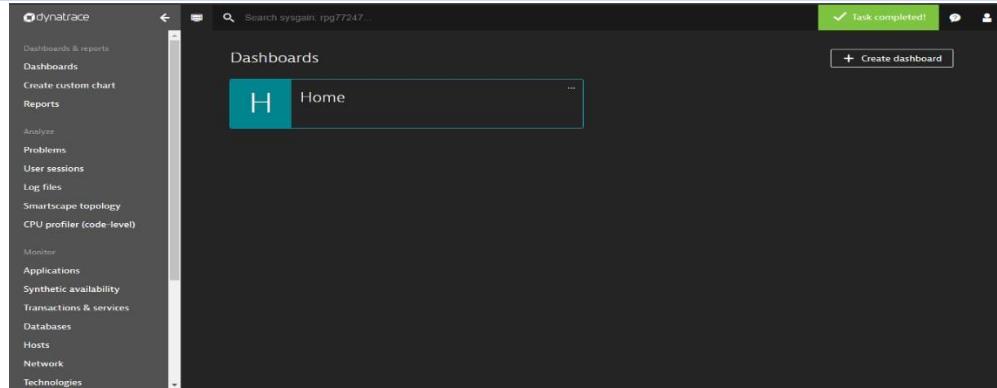
- restart service windows_service[Dynatrace OneAgent]
[2017-08-16T14:11:09+00:00] INFO: Chef Run complete in 22.297144 seconds

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"}]
```

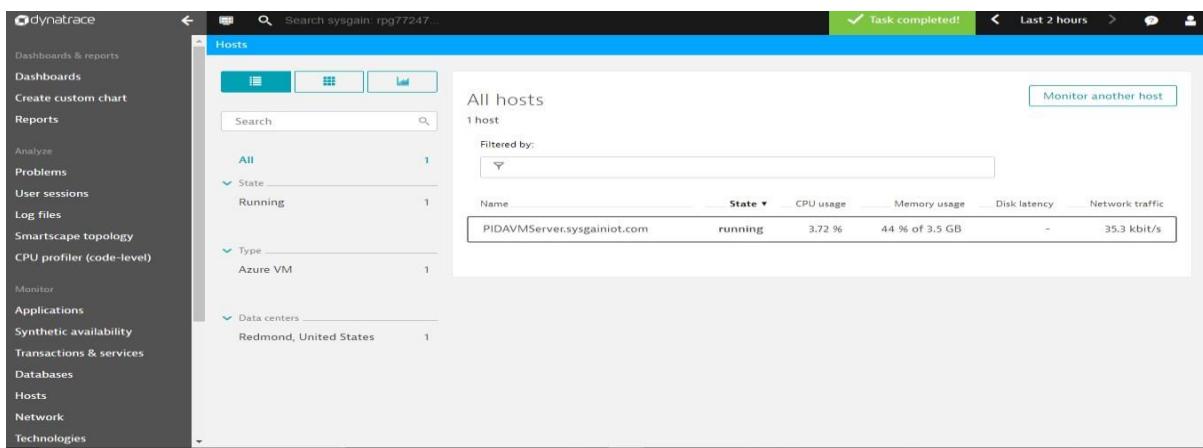
11. Go to the Dynatrace dashboard using the following URL: <https://www.dynatrace.com/>

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





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



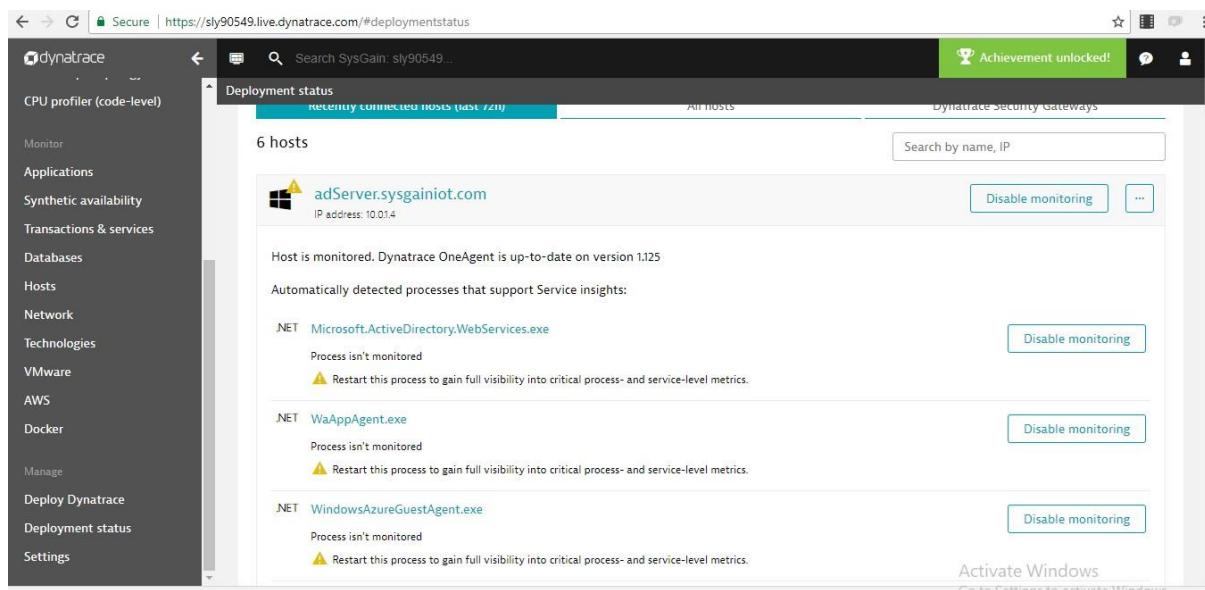
The screenshot shows the 'Hosts' page in Dynatrace. The left sidebar has the same navigation menu as the previous screenshot. The main area is titled 'Hosts' and shows a table for 'All hosts'. It displays one host entry:

Name	State	CPU usage	Memory usage	Disk latency	Network traffic
PIDAVMServer.sysgainiot.com	running	3.72 %	44 % of 3.5 GB	-	35.3 kbit/s

A 'Monitor another host' button is located in the top right of the host list area.

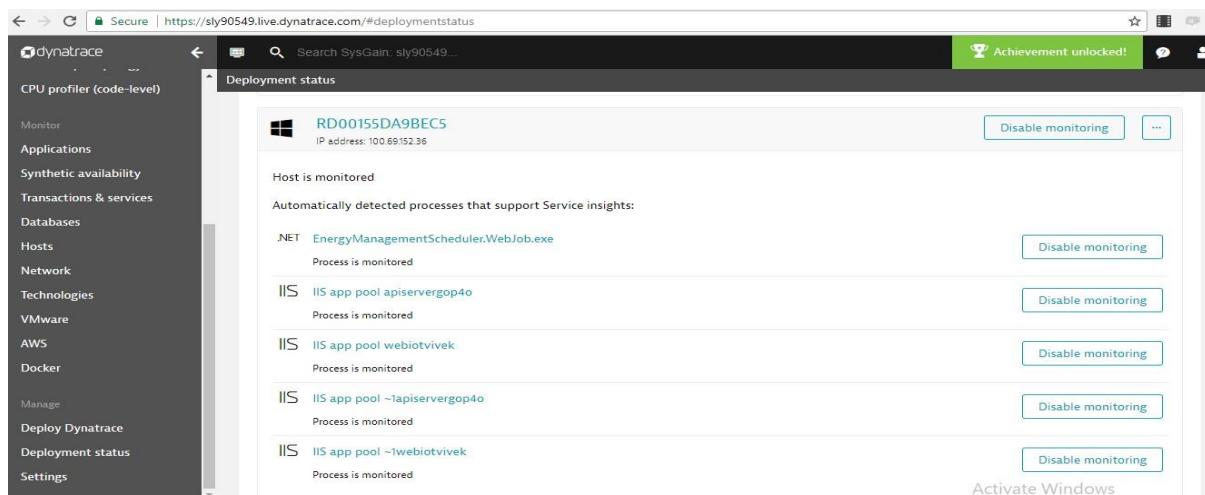
Navigate to **Deployment status** on the left pane of your dashboard page.

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



The screenshot shows the Dynatrace Deployment status page for the host `adServer.sysgainiot.com`. The host is monitored, and Dynatrace OneAgent is up-to-date on version 1.125. Three processes are listed as not monitored: `Microsoft.ActiveDirectory.WebServices.exe`, `WaAppAgent.exe`, and `WindowsAzureGuestAgent.exe`. Each process has a "Restart this process" button next to it.

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



The screenshot shows the Dynatrace Deployment status page for the host `RD00155DA9BEC5`. The host is monitored, and Dynatrace OneAgent is up-to-date on version 1.125. Five IIS app pools are listed as monitored: `EnergyManagementScheduler.WebJob.exe`, `IIS app pool apiservergop4o`, `IIS app pool webiotivivek`, `IIS app pool ~1apiservergop4o`, and `IIS app pool ~twebiotivivek`.

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 Hosts dashboard for PIDAVMServer.sysgainiot.com. The dashboard shows system health, resource usage, and process details.

Host Properties:

- Uptime: 1 day 1 hour 54 minutes
- Windows Server 2012 R2, ver. 6.3.9600
- CPU usage: 0.29 %
- Memory usage: 46 %
- Network: 1 NIC, 2 Disks

Availability: 100% Availability, 0 min total downtime.

Processes:

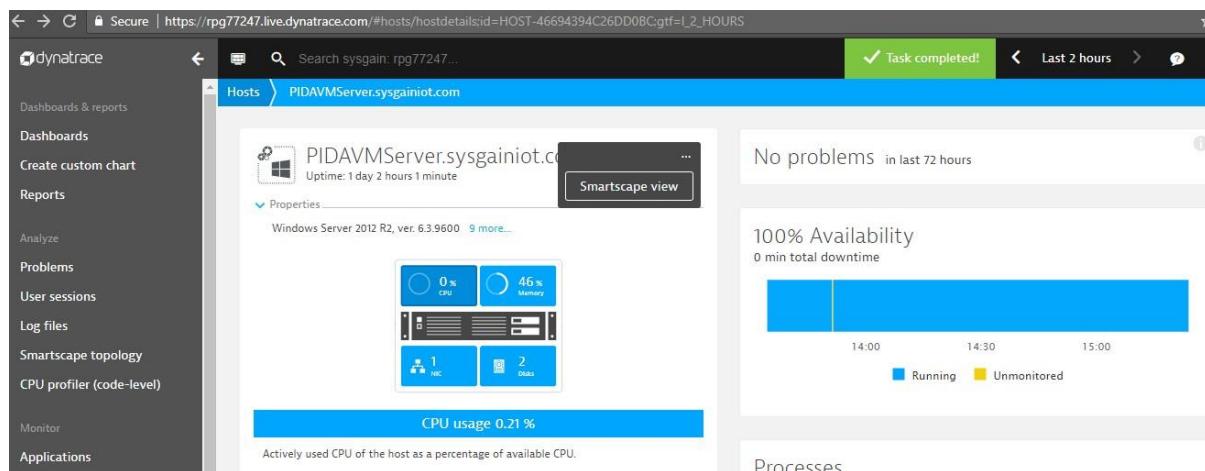
Process	Type	CPU	Memory	Traffic	Retransmissions	Connectivity
Deep Security Agent	Other	4.51 %	41.6 MB	-	-	-
OneAgent log analytics	Dynatrace	0.1 %	15.1 MB	4.74 kbit/s	0 %	100 %
Windows System	Windows	0.1 %	617 MB	4.84 kbit/s	3.6 %	100 %
ServerManager.exe	.NET	0 %	69.1 MB	-	-	-
OneAgent network monitoring	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 %

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

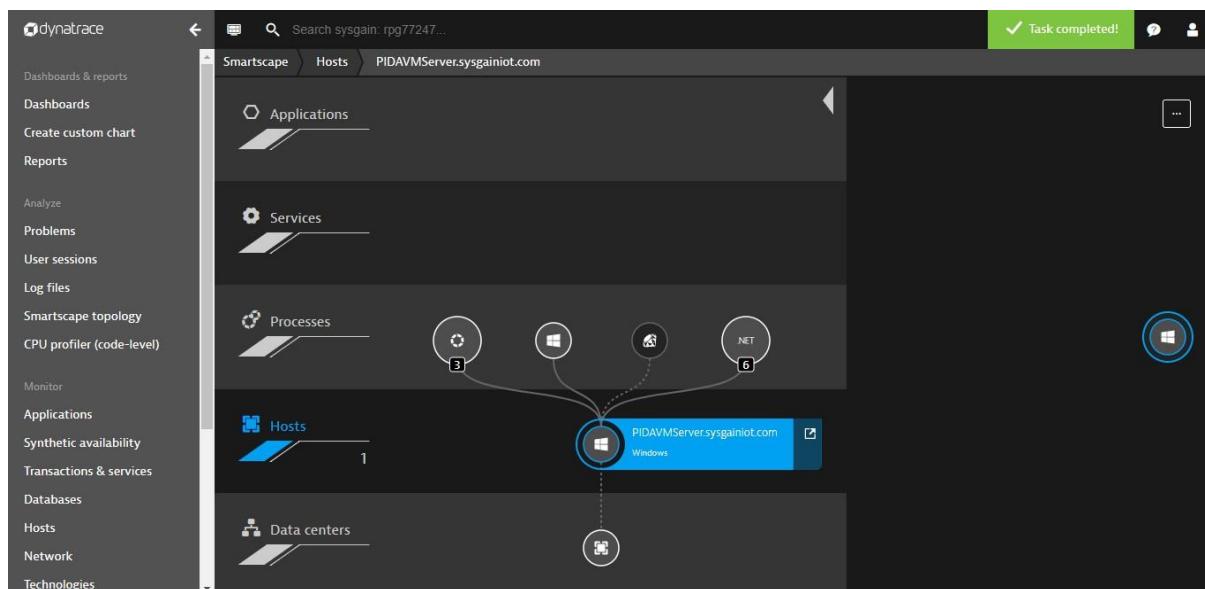
Screenshot of the Dynatrace Processes page for PIDAVMServer.sysgainiot.com. The page displays a list of running processes with their details.

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 links for 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, showing 'Uptime: 1 day 2 hours 1 minute' and 'Windows Server 2012 R2, ver. 6.3.9600'. It features a 'Smartscape view' button and a summary card with CPU usage (0.21%), Memory (46%), and Disk (1 HHD, 2 SSDs). A timeline chart shows '100% Availability' with 0 min total downtime from 14:00 to 15:00. A legend indicates 'Running' (blue) and 'Unmonitored' (yellow). Below the timeline is a section titled 'Processes'.



The screenshot shows the Dynatrace Smartscape topology page. The left sidebar lists categories such as Applications, Services, Processes, Hosts, and Data centers. The main area displays a network diagram where various components like applications, services, and processes are connected to a central host node labeled 'PIDAVMServer.sysgainiot.com Windows'. A circular icon with the number '6' is associated with one of the process nodes.

7.1.1. Installing Dynatraceoneagent To Web Application (PaaS Environment)

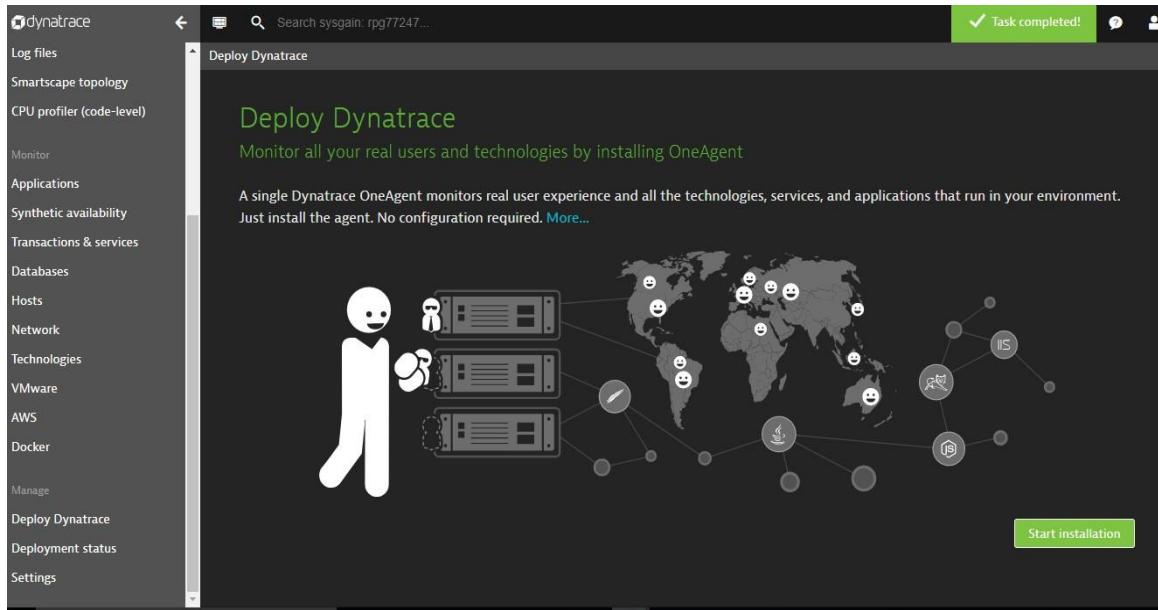
Azure Web Apps is a service provided by Microsoft Azure that gives you the option of deploying and auto-scaling applications and services. Using a predefined Azure site extension, you can modify your deployment by supplying additional resources or packages.

Generate a PaaS token:

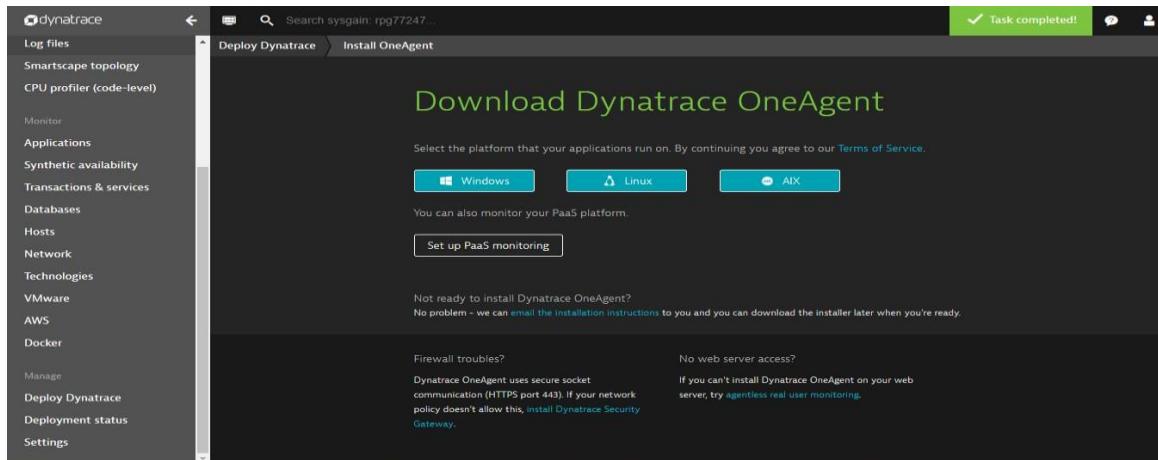
The first step is to get your environment ID and generate a PaaS token for your Dynatrace environment. This information is required so we can map your Azure account to your Dynatrace account.

To get your Dynatrace environment ID and PaaS token:

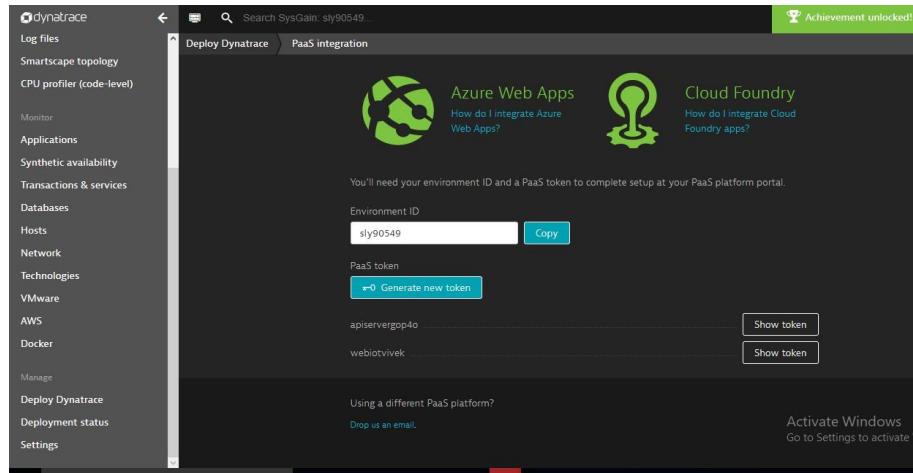
1. Login with your [Dynatrace account](#).
2. Select Deploy Dynatrace from the navigation menu.



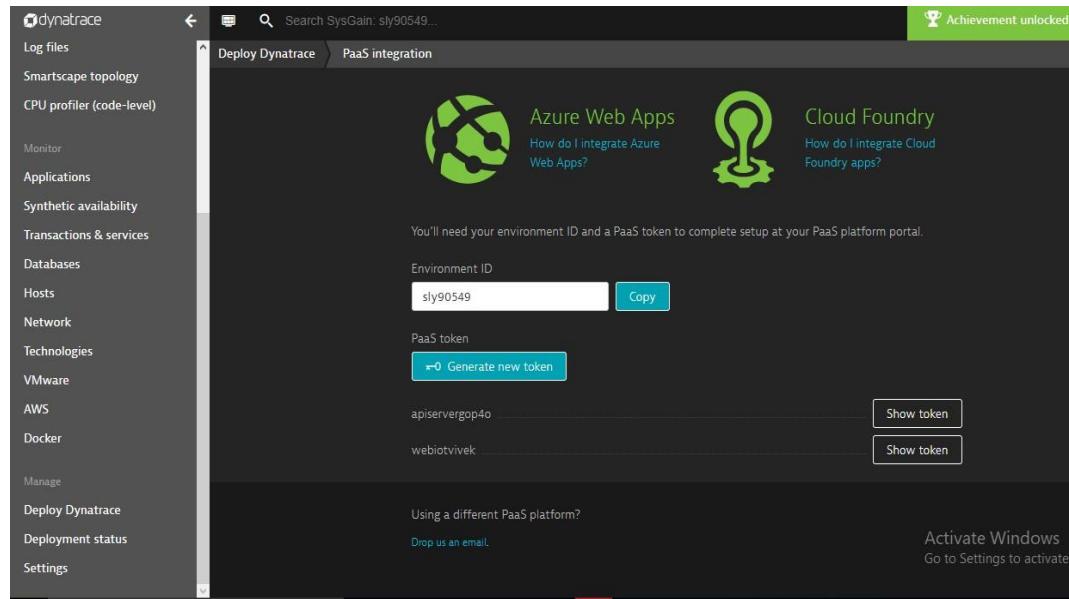
3. Click **Setup PaaS monitoring**.



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



- 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.

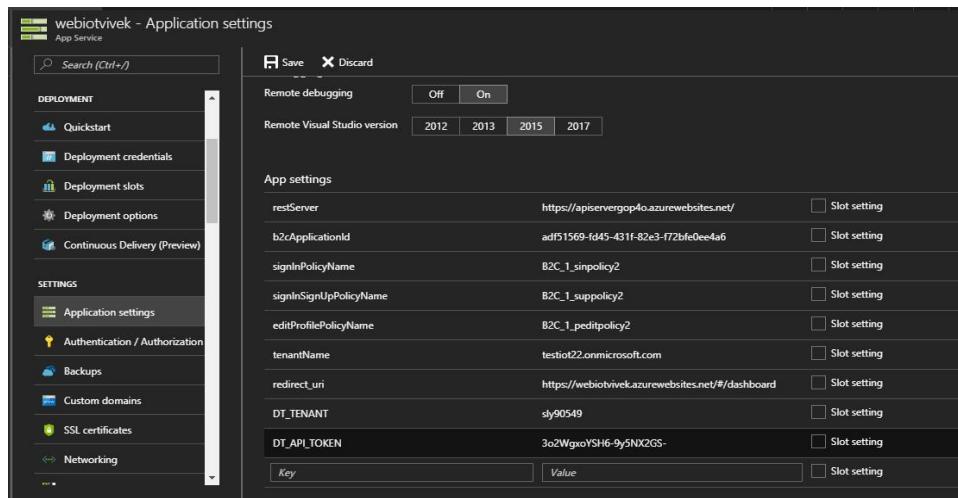


- Type in a meaningful name for your PaaS token. A meaningful token name might be the name of the PaaS platform you want to monitor (for example: azure, cloud-foundry, or openshift). To view and manage your existing PaaS tokens, go to **Settings > Integration > Platform as a Service**.
 - In the screenshots,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

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

Configure the Dynatrace Site Extension via the Azure portal

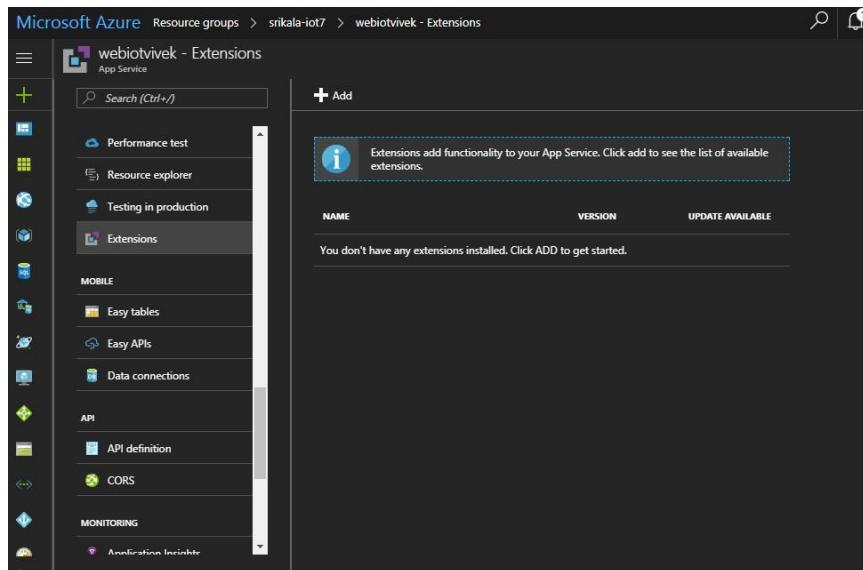
1. Now, open **portal.azure.com** in a new browser window.
 2. Navigate to the web app in the resource group you want to monitor.
 3. From **Settings**, select **Application Settings**. Then, scroll down to the App Settings area and add two new **Key/Value** pairs:
 4. **DT_TENANT**: Your environment ID, as shown above.
 5. **DT_API_TOKEN**: Copy and paste the PaaS token from the Download Dynatrace page shown above.
- <https://help.dynatrace.com/images/content/infrastructuremonitoring/paas/portal.png>.



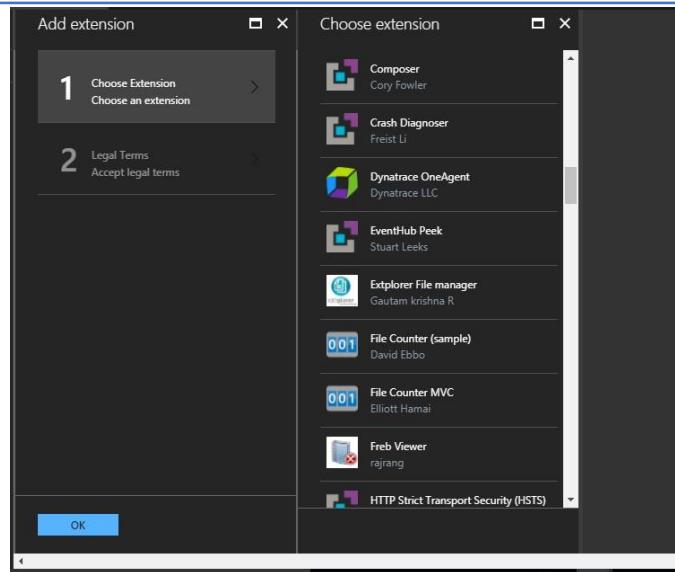
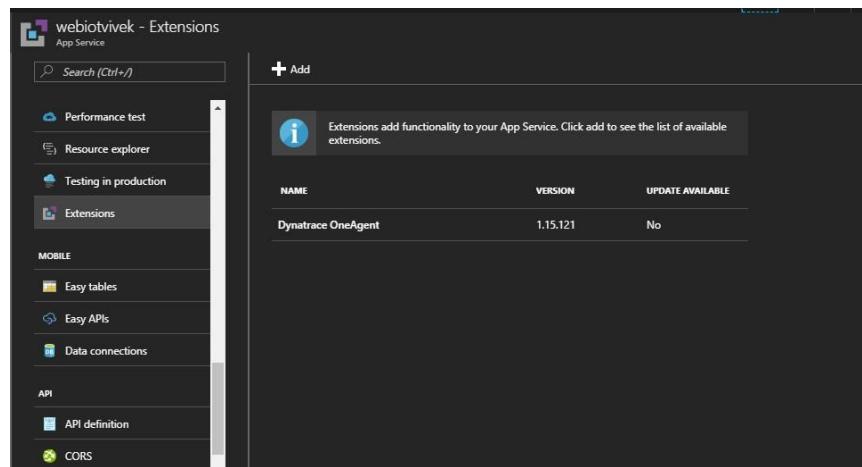
Install the Dynatrace Azure site extension

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 righthand side, click **Add**.



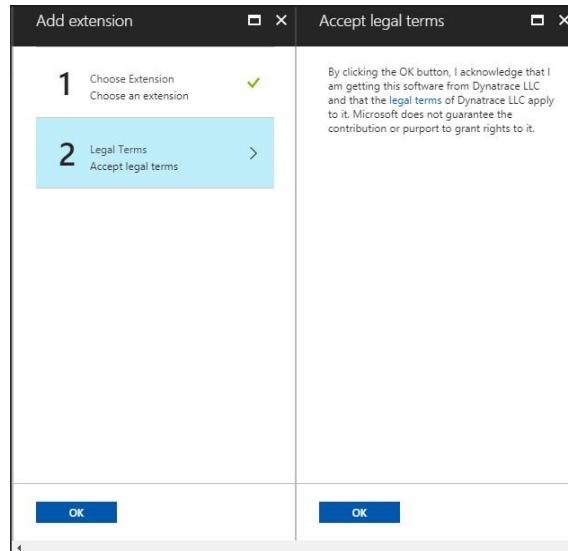
5. Scroll through the list until you find **Dynatrace OneAgent**. Note that entries are not ordered alphabetically.
<https://help.dynatrace.com/images/content/infrastructuremonitoring/paas/extension.png>

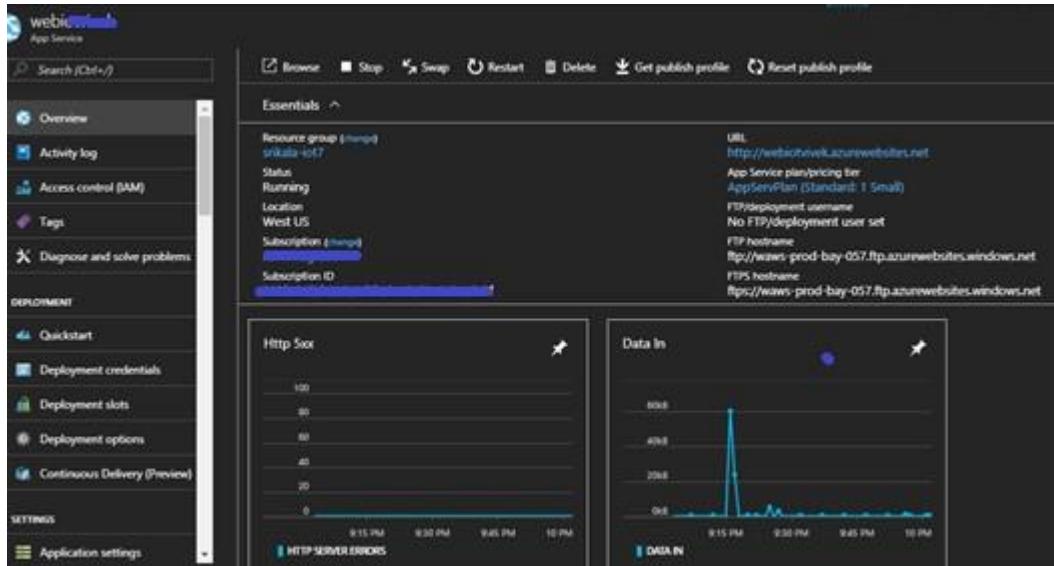
The image shows the 'Extensions' blade in the Azure portal. The left sidebar includes 'Performance test', 'Resource explorer', 'Testing in production', 'Extensions' (which is selected), 'Easy tables', 'Easy APIs', 'Data connections', 'API definition', and 'CORS'. The main area has a search bar and a message: 'Extensions add functionality to your App Service. Click add to see the list of available extensions.' Below is a table:

NAME	VERSION	UPDATE AVAILABLE
Dynatrace OneAgent	1.15.121	No

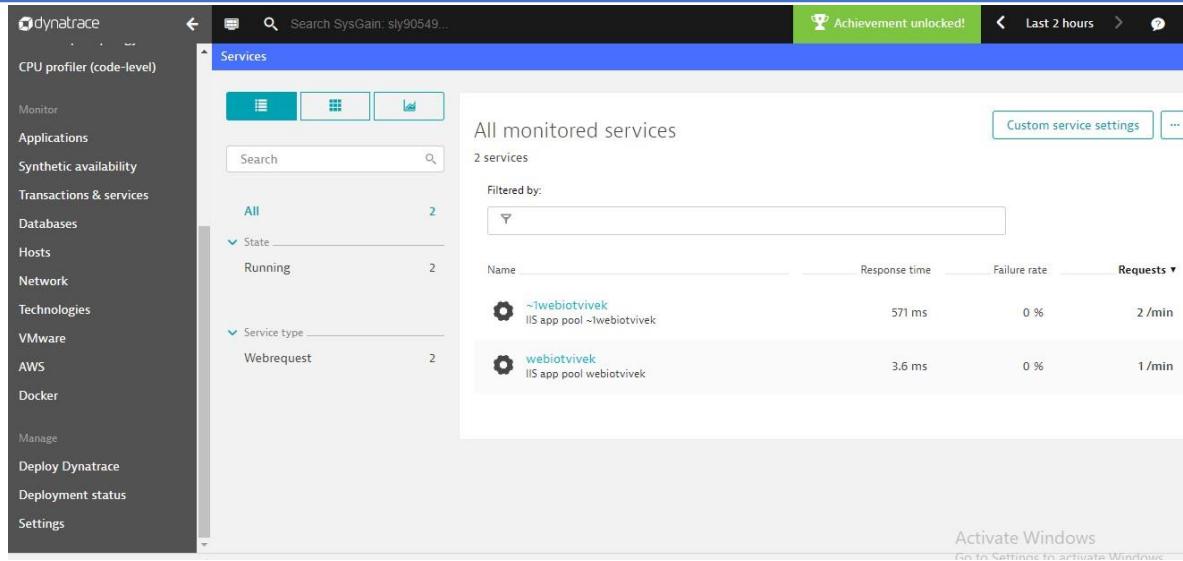
- Click **OK** to apply Dynatrace monitoring to your Azure website.



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.

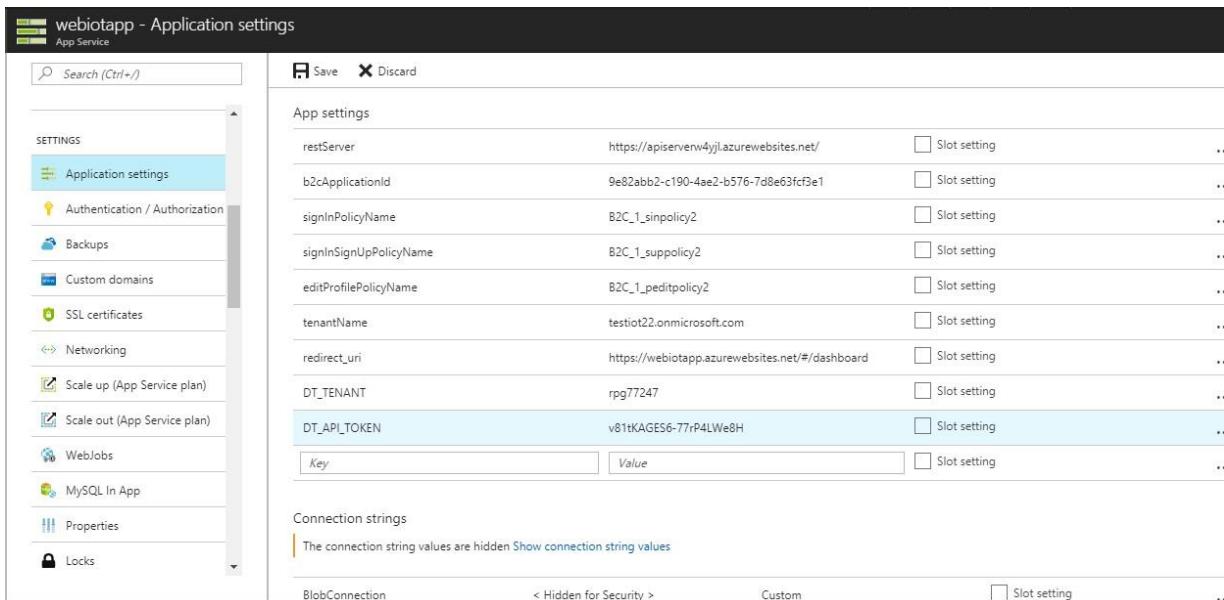


8. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added



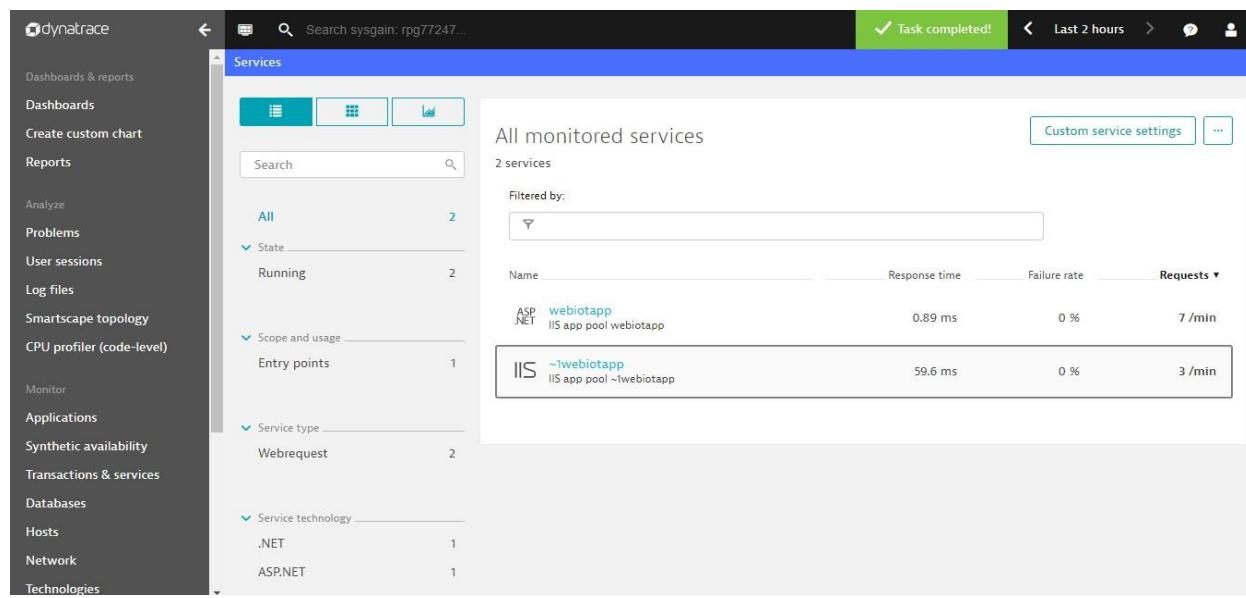
The screenshot shows the Dynatrace interface. On the left, a sidebar lists various monitoring categories like CPU profiler, Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main area is titled 'Services' and displays 'All monitored services'. It shows 2 services: '~1webiotvivek' (IIS app pool ~1webiotvivek) with a response time of 571 ms, failure rate of 0 %, and requests per minute at 2/min; and 'webiotvivek' (IIS app pool webiotvivek) with a response time of 3.6 ms, failure rate of 0 %, and requests per minute at 1/min. A green banner at the top right says 'Achievement unlocked! Last 2 hours'.

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



The screenshot shows the 'Application settings' blade for the 'webiotapp' App Service. The left sidebar includes options like SETTINGS (selected), Application settings (highlighted), Authentication / Authorization, Backups, Custom domains, SSL certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), WebJobs, MySQL In App, Properties, and Locks. The main area shows 'App settings' with several key-value pairs: restServer (https://apiservenv4yj.azurewebsites.net/), b2cApplicationId (9e82abb2-c190-4ae2-b576-7d8e63fcf3e1), signInPolicyName (B2C_1_sinpolicy2), signInSignUpPolicyName (B2C_1_supolicy2), editProfilePolicyName (B2C_1_peditpolicy2), tenantName (testiot22.onmicrosoft.com), redirect_uri (https://webiotapp.azurewebsites.net/#/dashboard), DT_TENANT (rpg77247), and DT_API_TOKEN (v81tKAGES6-77rP4LWe8H). Below this is a 'Connection strings' section with a note: 'The connection string values are hidden Show connection string values'. At the bottom, there are tabs for BlobConnection, < Hidden for Security >, Custom, and a 'Slot setting' checkbox.

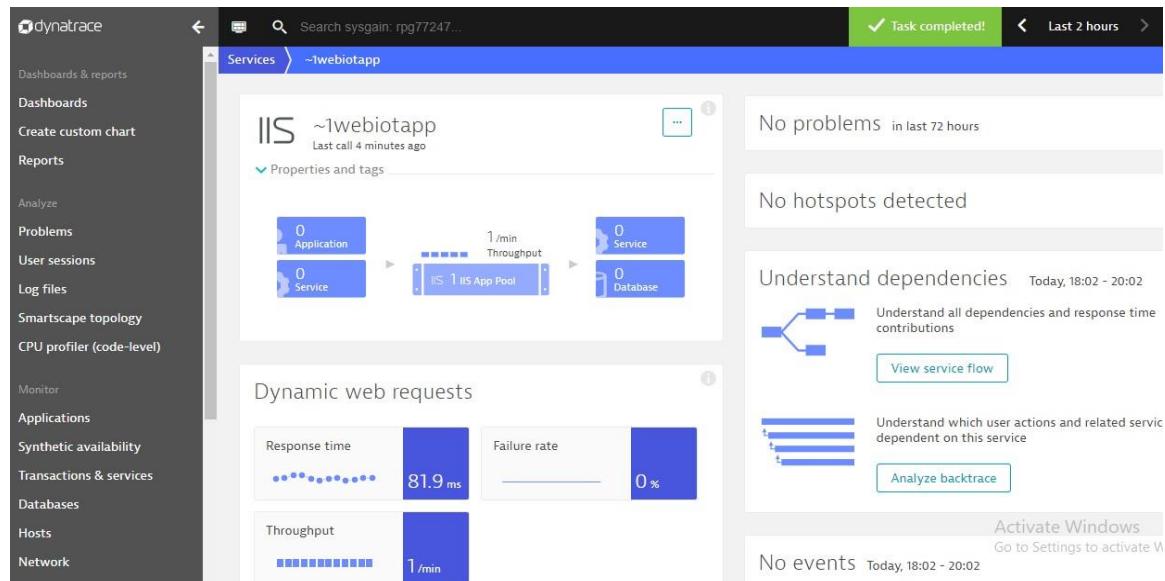
10. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added.



The screenshot shows the Dynatrace Services dashboard. On the left, a sidebar lists various monitoring categories. The main area displays a list of 'All monitored services' with two entries:

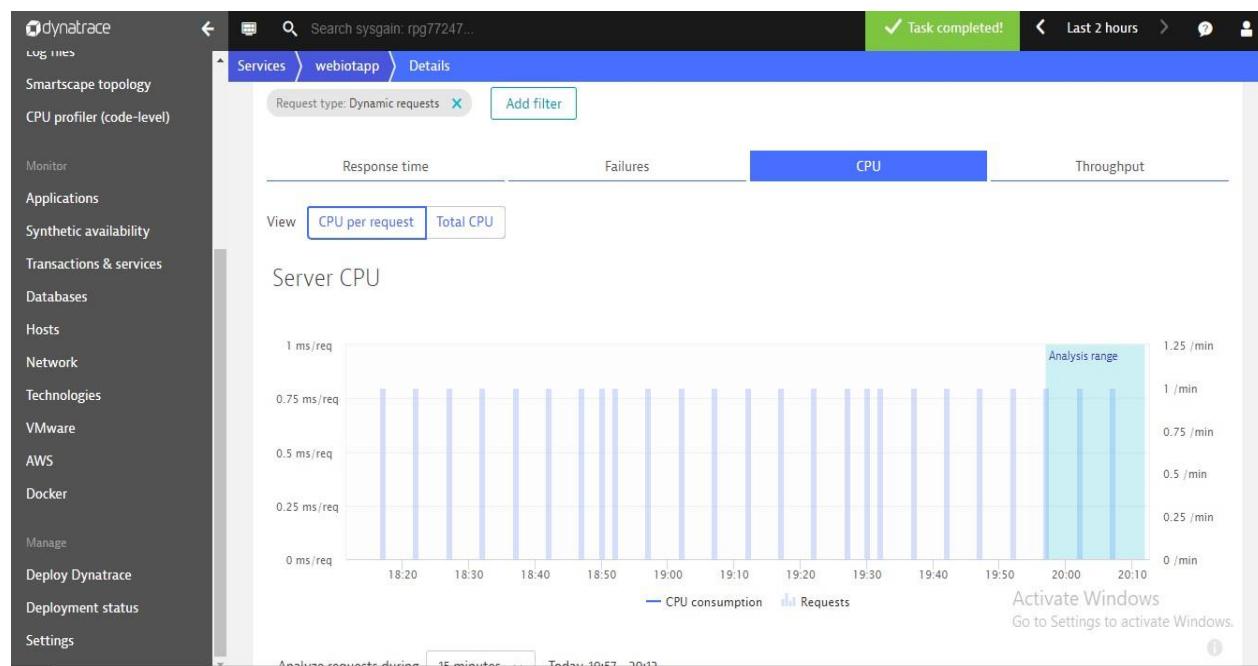
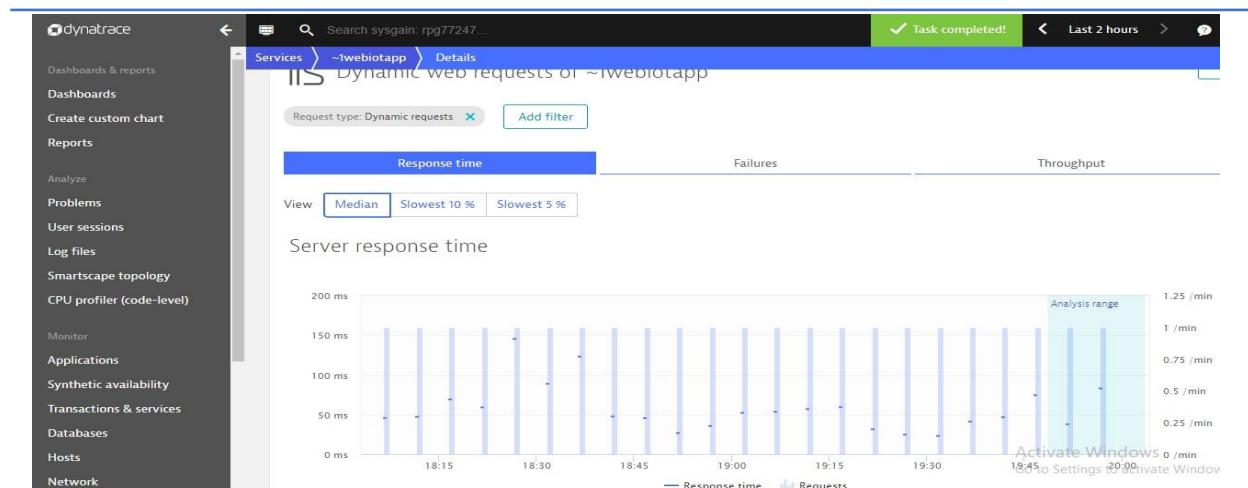
- ASP .NET webiotapp**: IIS app pool webiotapp. Response time: 0.89 ms, Failure rate: 0 %, Requests: 7 /min.
- IIS ~!webiotapp**: IIS app pool ~!webiotapp. Response time: 59.6 ms, Failure rate: 0 %, Requests: 3 /min.

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 is identical to the previous dashboard. The main area includes:

- Properties and tags**: Shows 0 Application, 0 Service, 1/min Throughput, and 0 Database.
- Dynamic web requests**: Shows Response time (81.9 ms), Failure rate (0 %), and Throughput (1 /min).
- No problems in last 72 hours**
- No hotspots detected**
- Understand dependencies**: Shows a dependency graph with 'IIS' at the center, connected to 'IIS App Pool' and 'Database'. A callout says 'Understand all dependencies and response time contributions' with a 'View service flow' button.
- Analyze backtrace**: Shows a stack trace diagram with a callout 'Understand which user actions and related services dependent on this service'.
- No events**: Shows 'No events' from 'Today, 18:02 - 20:02'.



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

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
- Settings

Search sysgain: rpg77247...

Task completed! Last 2 hours

Services > webiotapp Properties and tags

No hotspots detected

Understand dependencies Today, 18:18 - 20:18

Understand all dependencies and response time contributions

View service flow

Dynamic web requests

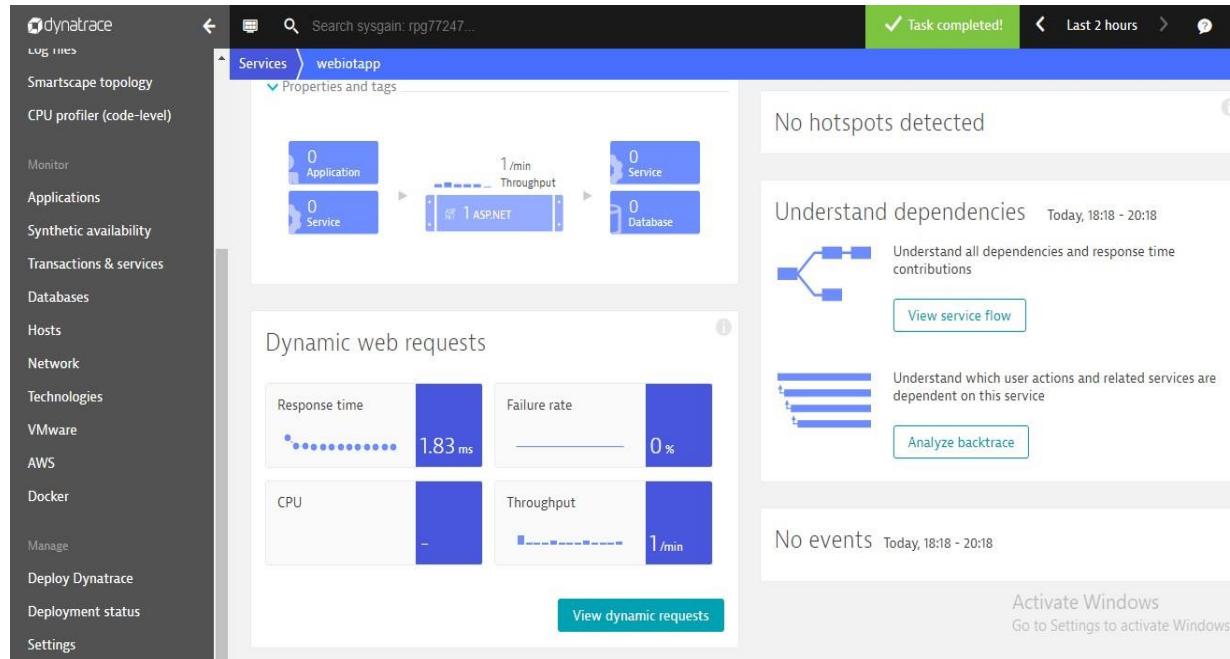
Response time: 1.83 ms Failure rate: 0 %

CPU: - Throughput: 1/min

View dynamic requests

No events Today, 18:18 - 20:18

Activate Windows Go to Settings to activate Windows



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
- Settings

Search sysgain: rpg77247...

Task completed!

Services > webiotapp > Details > Service flow

Showing service flow of requests to 'webiotapp'

Today, 18:18 - 20:18 (2 Hours) Apply

Add filter

NET webiotapp

Avg. response time: 779 ms Requests: 26 Failed requests: 0

See every single request in PurePath view

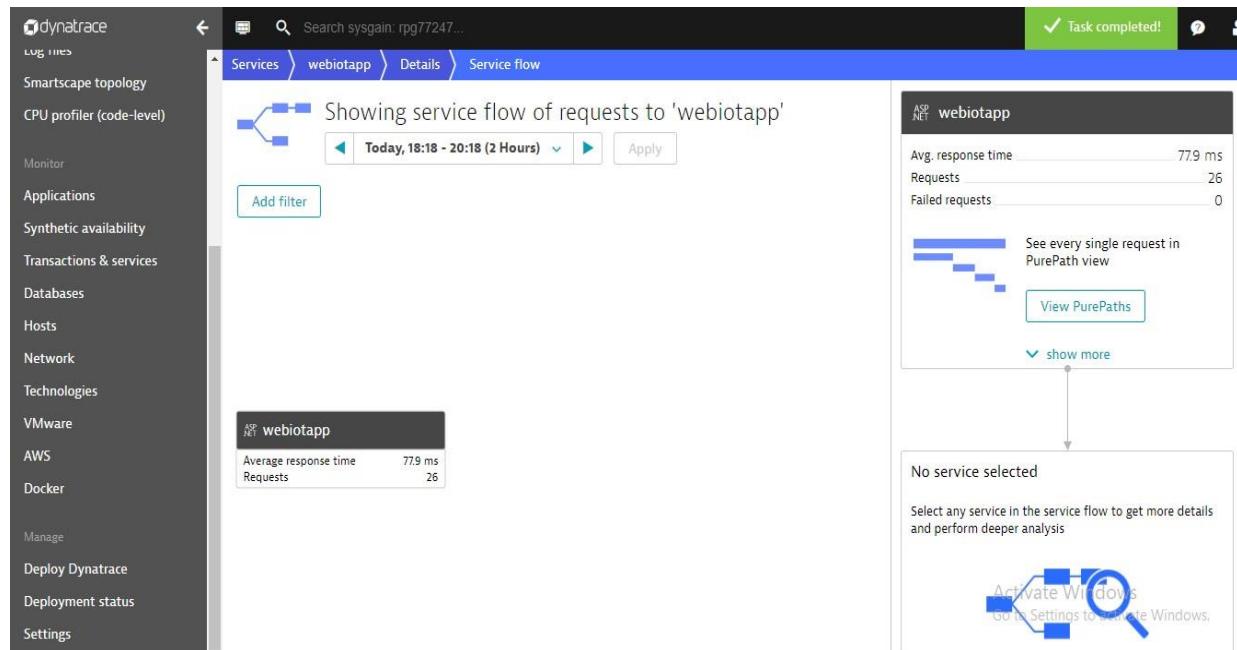
View PurePaths

show more

No service selected

Select any service in the service flow to get more details and perform deeper analysis

Activate Windows Go to Settings to activate Windows



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

The screenshot shows the Sysgain dashboard interface. The top navigation bar includes links for 'dynatrace', 'Logs & Metrics', 'Smartscape topology', 'CPU profiler (code-level)', 'Monitor', 'Applications', 'Synthetic availability', 'Transactions & services', 'Databases', 'Hosts', 'Network', 'Technologies' (with options for 'VMware', 'AWS', 'Docker'), 'Manage', 'Deploy Dynatrace', 'Deployment status', and 'Settings'. A search bar at the top right contains the text 'Search sysgain: rpg77247...'. Below the search bar, a breadcrumb navigation path shows 'Services > webiotapp > Details > Backtrace'. A green banner at the top right indicates 'Task completed!'. The main content area displays a 'Service-level backtrace of requests to 'webiotapp'' with a timeline from 'Today, 18:20 - 20:20 (2 Hours)'. It includes a 'Add filter' button and a section titled 'Incoming requests to this service' showing a call tree with nodes like 'ASP .NET webiotapp' and 'IIS app pool webiotapp'. A progress bar indicates '26 Requests' with '0 Failed requests'. In the bottom right corner, there is a message: 'Activate Windows Go to Settings to activate Windows'.

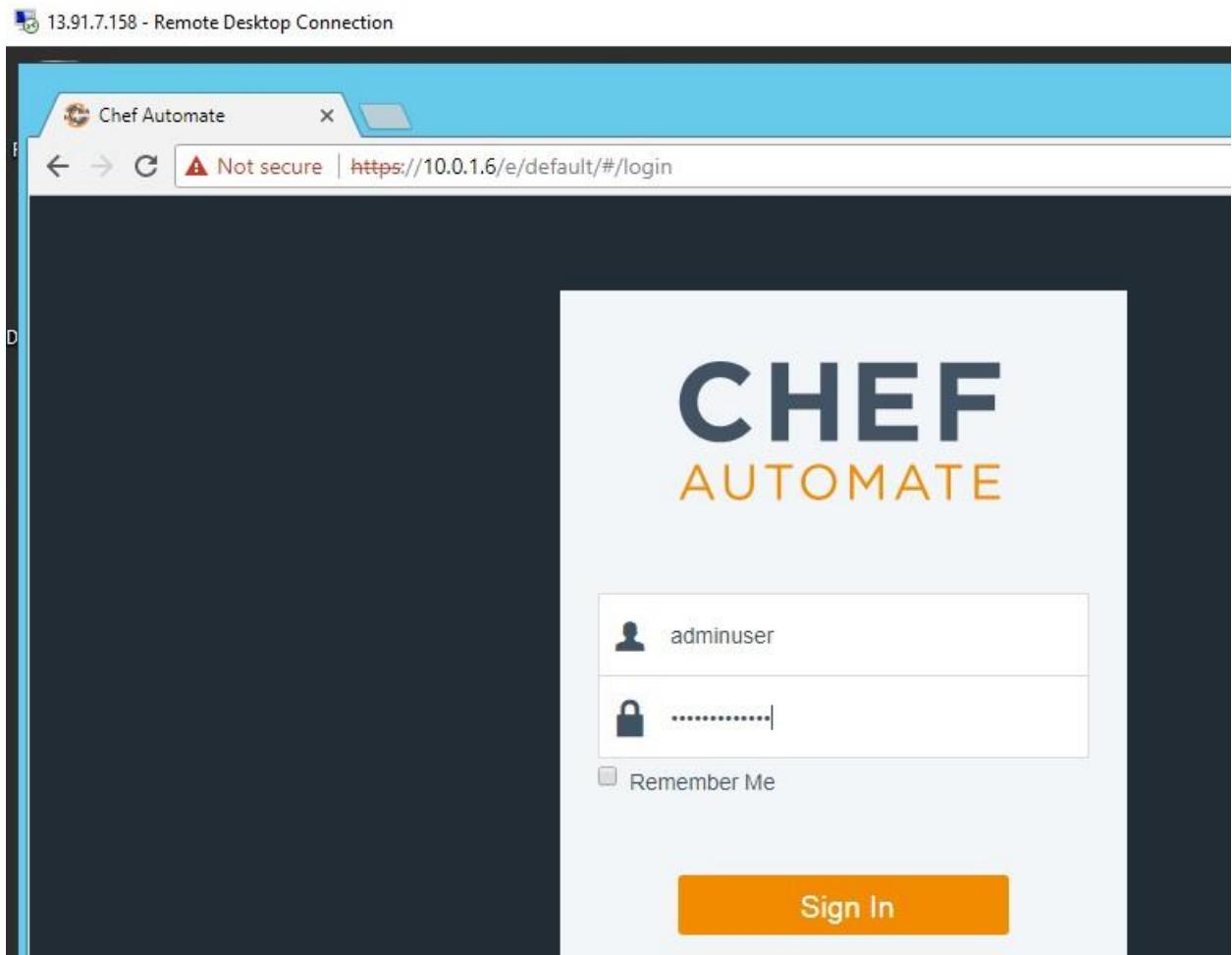
7.2. Chef Automate

To check the installed nodes status.

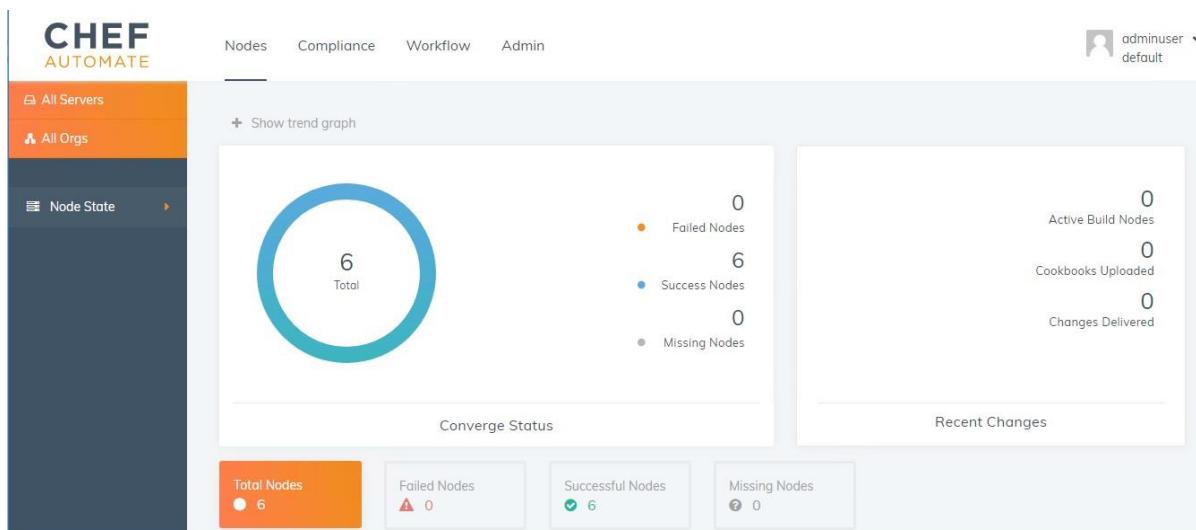
1. Using **workstationFQDN**, Login to the ChefWorkStation with **adminUsername** provided in the outputs section and password as **adminPassword** used during template deployment.



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.



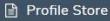
-  All Servers
-  All Orgs
-  Node State

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 noncompliance.

 Reporting

 Profile Store

Your System is Compliant

[Report Metadata](#)

Overview
6 Nodes
2 Profiles

Node Status
Profile Status



6
Total Nodes

0
Failed Nodes

6
Passed Nodes

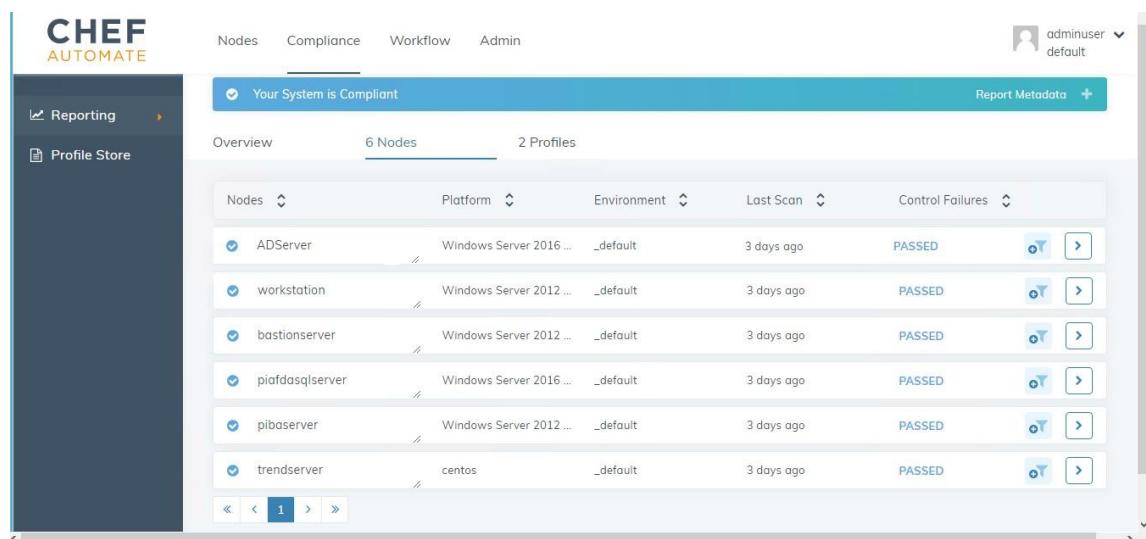
0
Skipped Nodes

0
CRITICAL

0
MAJOR

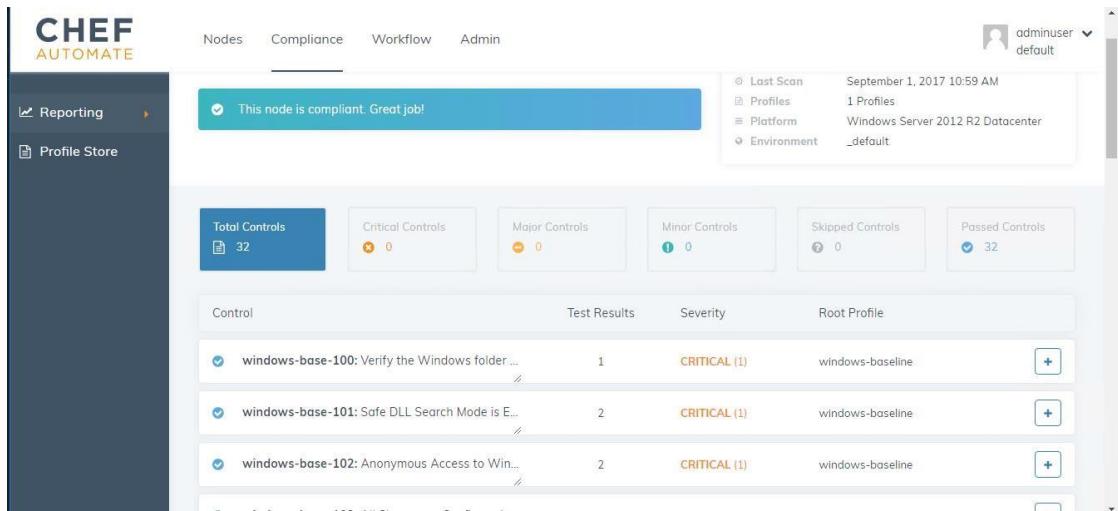
0
MINOR

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



The screenshot shows the Chef Automate interface under the 'Reporting' section. At the top, there are tabs for Nodes, Compliance, Workflow, and Admin. A user profile is shown on the right. The main area displays a message: 'Your System is Compliant'. Below this, there are two tabs: 'Overview' and '6 Nodes' (which is selected). Underneath, a table lists six nodes: ADServer, workstation, bastionserver, piafdasqlserver, pibaserver, and trendserver. Each node entry includes its name, platform, environment, last scan date, control failures status (all are PASSED), and a 'View Details' button.

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



This screenshot shows the same Chef Automate interface for a specific node. The message at the top says 'This node is compliant. Great job!'. On the right, there are filter options for Last Scan (September 1, 2017 10:59 AM), Profiles (1 Profiles), Platform (Windows Server 2012 R2 Datacenter), and Environment (_default). Below this, a summary bar shows 'Total Controls: 32', 'Critical Controls: 0', 'Major Controls: 0', 'Minor Controls: 0', 'Skipped Controls: 0', and 'Passed Controls: 32'. The main table lists three controls with the following details:

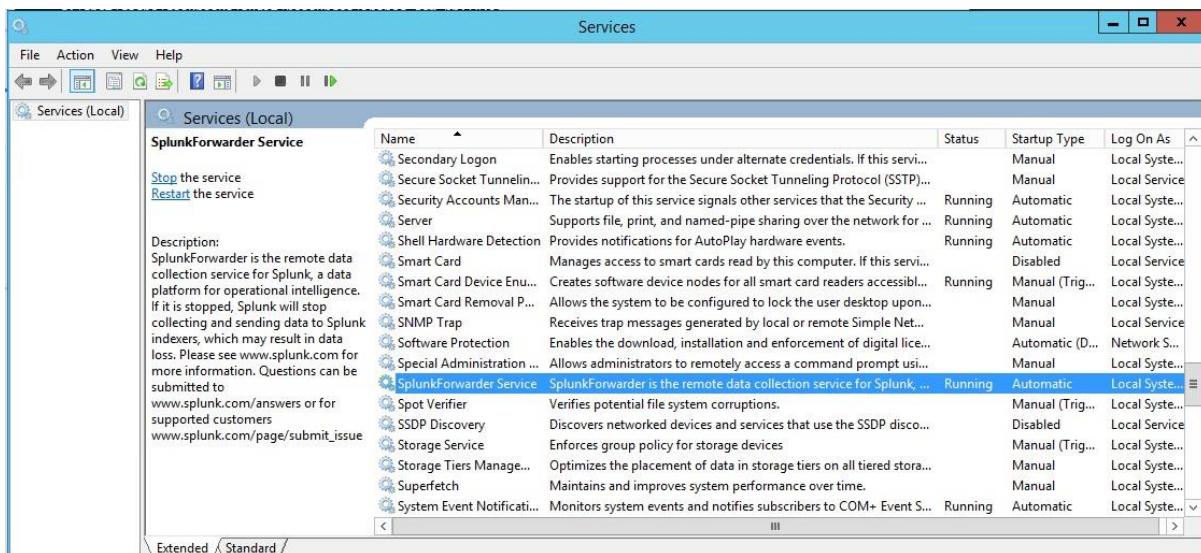
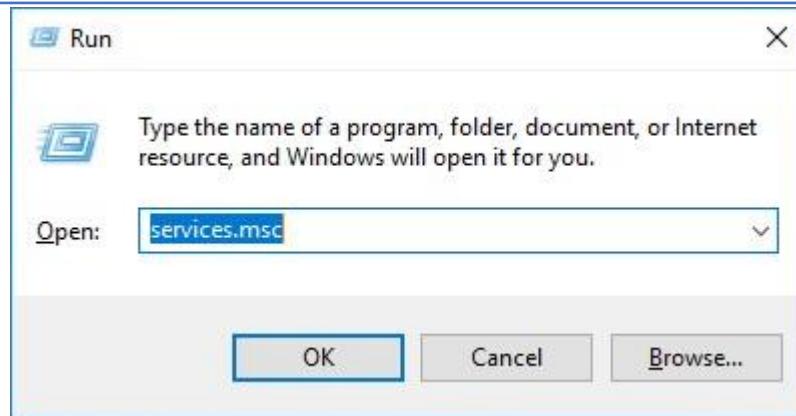
Control	Test Results	Severity	Root Profile
windows-base-100: Verify the Windows folder ...	1	CRITICAL (1)	windows-baseline
windows-base-101: Safe DLL Search Mode is E... windows-base-102: Anonymous Access to Win...	2	CRITICAL (1)	windows-baseline
windows-base-102: Anonymous Access to Win...	2	CRITICAL (1)	windows-baseline

Splunk Universal Forwarder Installation Using Chef Automate:

Splunk universal Forwarder software is used to forward the windows 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 event logs to the splunk server.

Checking the Splunk forwarder installation status in client server:

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



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

7.3. Splunk

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

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

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



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



splunk > App: Search & Reporting

Administrator > Messages > Settings > Activity > Help > Find

Search Datasets Reports Alerts Dashboards Search & Reporting

Q. Search enter search here... Last 24 hours < Smart Mode

No Event Sampling

How to Search If you are not familiar with the search features, or want to learn more, see one of the following resources.

Documentation Tutorial

What to Search 585,582 Events INDEXED a month ago EARLIEST EVENT a few seconds ago LATEST EVENT

Data Summary

Search History > Expand your search history

About Support File a Bug Documentation Privacy Policy © 2005-2017 Splunk Inc. All rights reserved.

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

splunk > App: Search & Reporting

Administrator > Messages > Settings > Activity > Help > Find

Search Datasets Reports Alerts Dashboards Search & Reporting

Q. Search host="bastionserver" Last 24 hours < Smart Mode

No Event Sampling

How to Search If you are not familiar with the search features, or want to learn more, see one of the following resources.

Documentation Tutorial

What to Search 129,781 Events INDEXED a month ago EARLIEST EVENT a few seconds ago LATEST EVENT

Data Summary

Search History > Expand your search history

Search Datasets Reports Alerts Dashboards Search & Reporting

Q. New Search host="bastionserver" Last 24 hours < Smart Mode

✓ 60,616 events (8/29/17 12:00:00.000 PM to 8/30/17 12:21:27.000 PM) No Event Sampling

Events (60,616) Patterns Statistics Visualization Job < Zoom Out + Zoom to Selection × Deselect 1 hour per column

Format Timeline < Zoom Out + Zoom to Selection × Deselect 1 hour per column

List < Hide Fields All Fields Time Event

	Time	Event
>	8/30/17 12:21:25.000 PM	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
>	8/30/17 12:21:04.000 PM	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

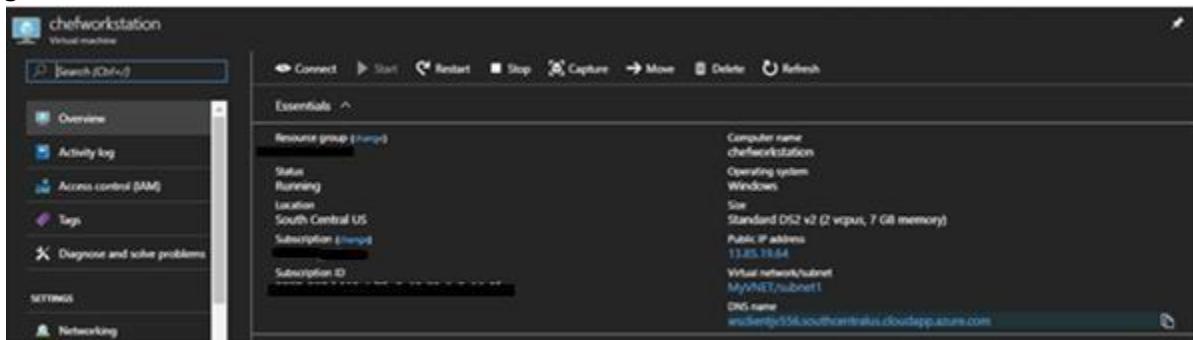
< Prev 1 2 3 4 5 6 7 8 9 ... Next >

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

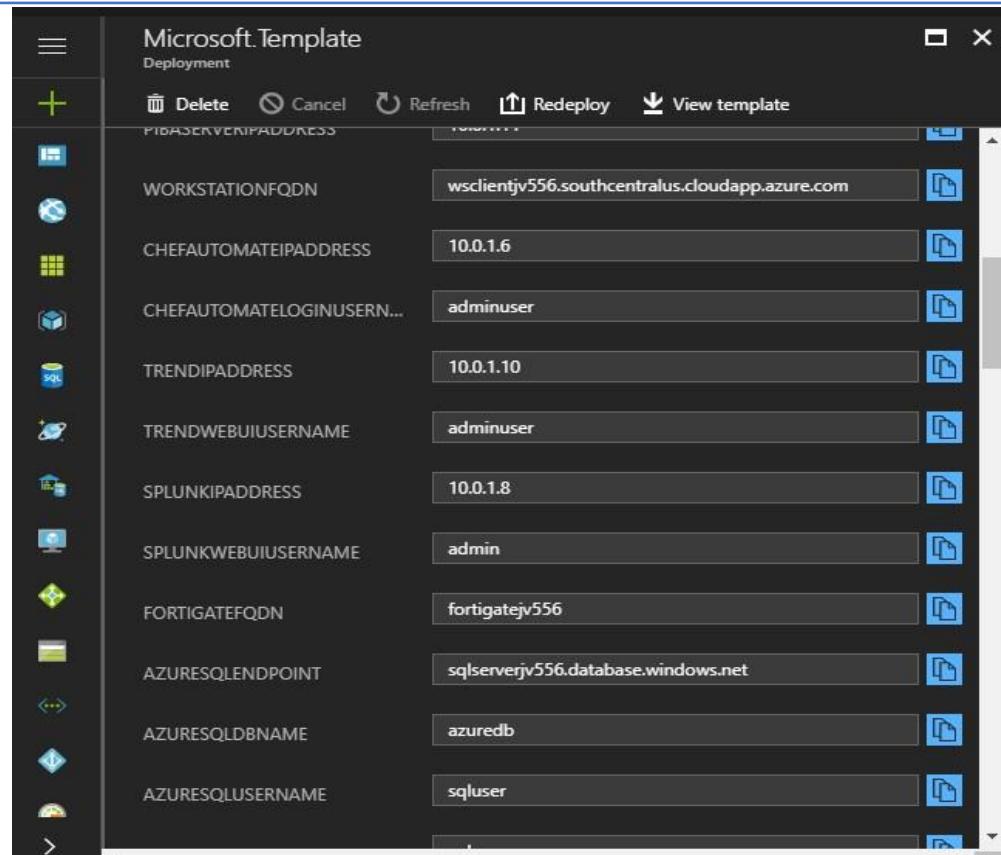
7.4. TrendMicro

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

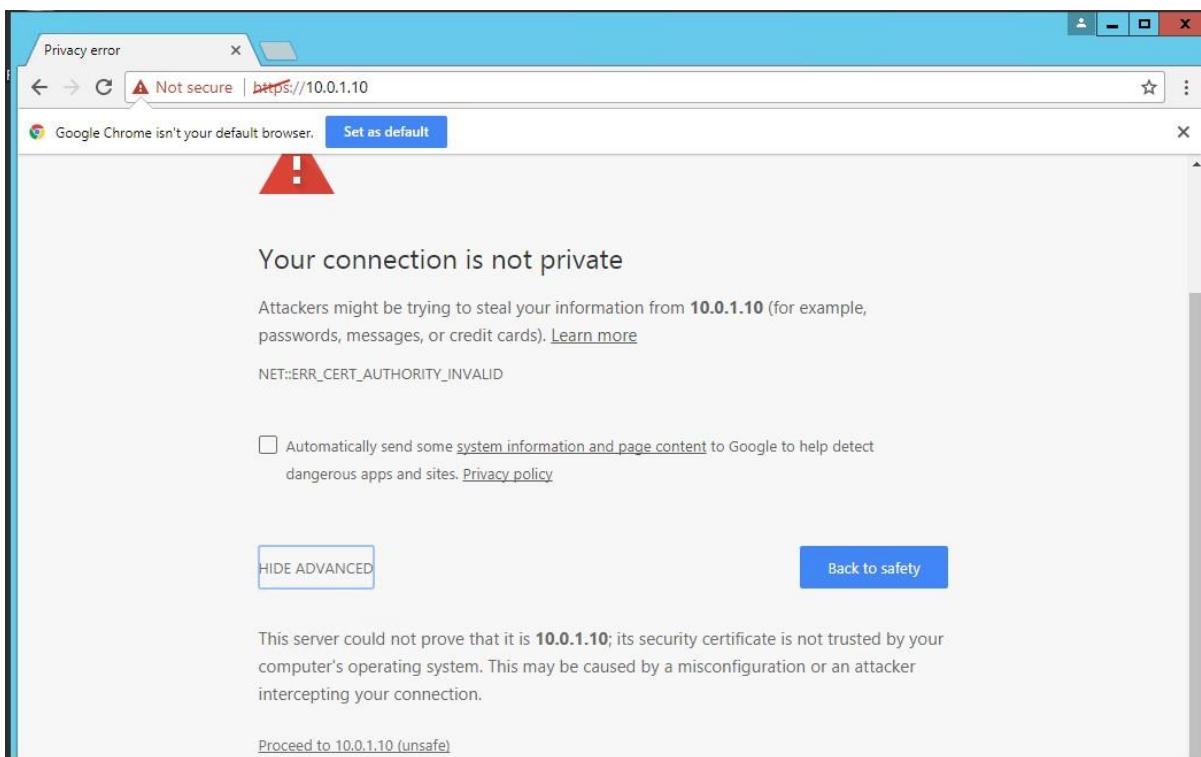
Login to Bastion Host or ChefWorkstation server.



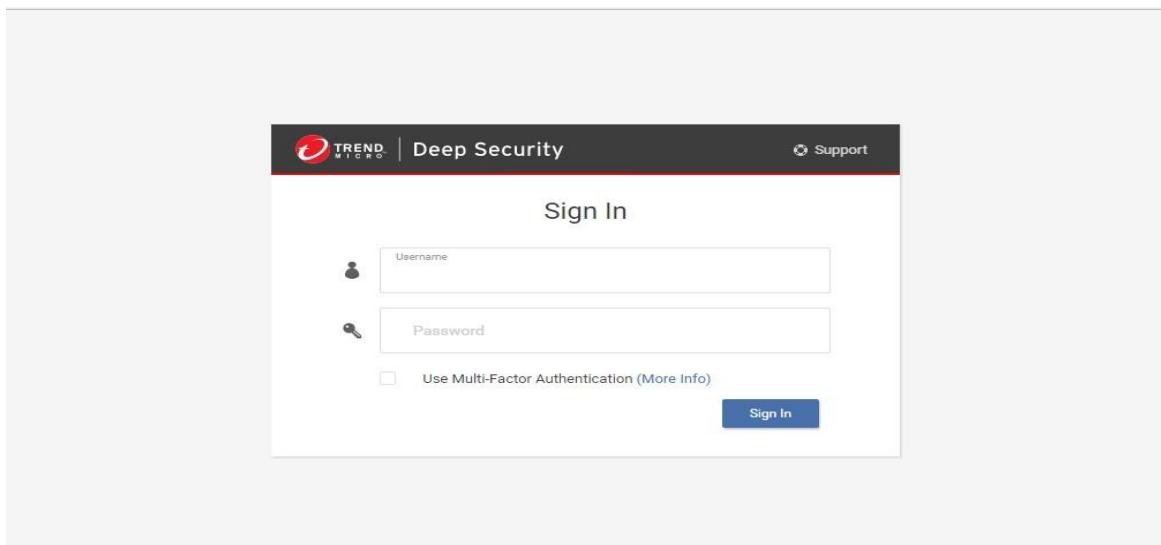
Once login open Browser and enter the TrendMicro IP address, which we get from output section of IOT ARM Template.



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.

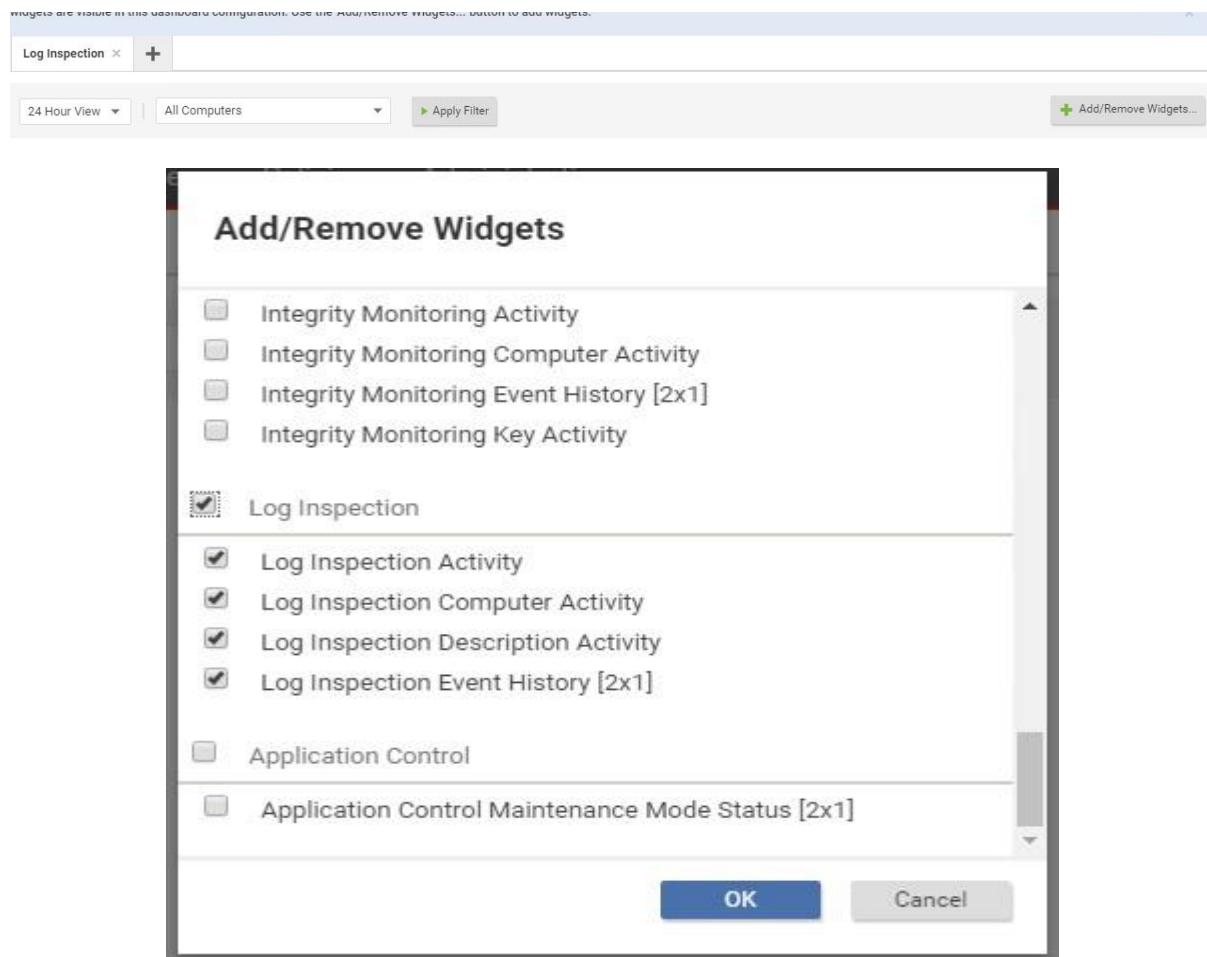
The screenshot shows the Trend Micro Deep Security dashboard. At the top, there's a navigation bar with the Trend Micro logo, 'Deep Security', user info ('adminuser'), and a search bar. Below the navigation is a main header with tabs: 'Dashboard' (selected), 'Actions', 'Alerts', 'Events & Reports', 'Computers', 'Policies', and 'Administration'. Underneath this is a toolbar with buttons for 'Default' and '+ Add/Remove Widgets...'. The dashboard 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:** A large green circle indicating 8 Managed computers. A smaller table shows the status distribution: 0 Critical, 0 Warning, 8 Managed, and 0 Unmanaged.
- My User Summary:** Details for user 'adminuser': ROLE Full Access, LAST SIGN-IN August 31, 2017 12:28, and PREVIOUS SIGN-IN N/A.
- Ransomware Status:** Shows 0 Ransomware instances.
- Ransomware Event History:** An empty table.

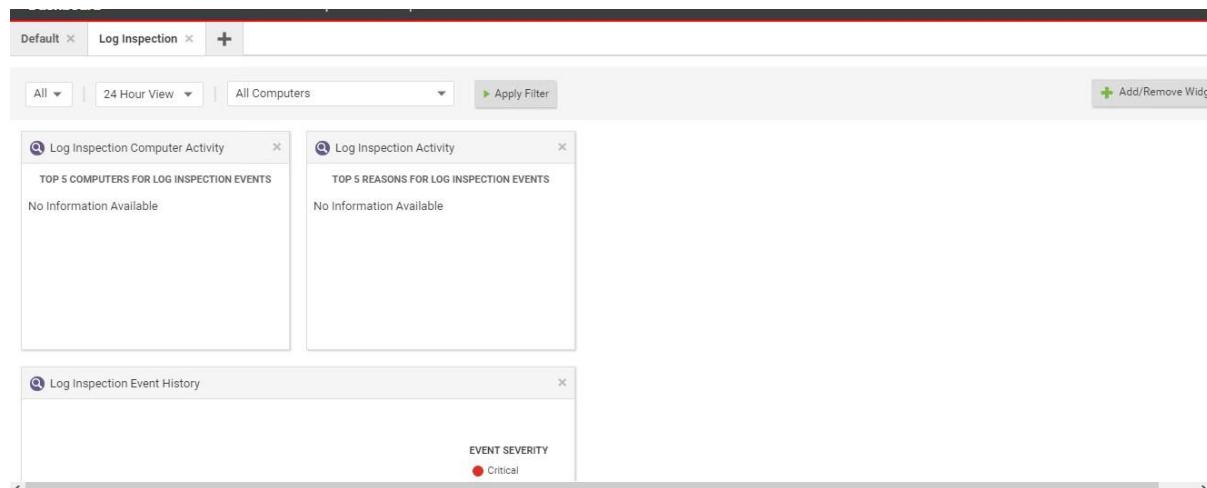
We can create our own Dashboard by clicking on "+" icon Besides Default and add the Widgets which you want to monitor.

The screenshot shows the 'Add New Dashboard' dialog box. It has fields for 'New Dashboard Name:' (containing 'Log Inspection') and 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 the Trend Micro logo, "Deep Security", user information ("adminuser"), and links for "News", "Help", "Support", and "Help Center Search". Below the navigation is a secondary menu with "Dashboard", "Actions", "Alerts", "Events & Reports", "Computers" (which is highlighted in blue), "Policies", and "Administration". On the left, a sidebar lists "Smart Folders" and "Computers" (also highlighted in blue). The main content area is titled "Computers" with filters "With sub-Groups" and "By Group". It features a toolbar with "Add", "Delete...", "Details...", "Actions", "Events", "Export", and "Columns...". A table lists 8 computers, each with a small icon, name, platform, policy, status, and maintenance info. All listed computers are "Managed (Online)" with "N/A" for maintenance.

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
10.0.1.14		Microsoft Win...	None	Managed (Online)	N/A
10.0.1.15		Microsoft Win...	None	Managed (Online)	N/A
10.0.1.16		Ubuntu Linux ...	None	Managed (Online)	N/A
10.0.1.18		Ubuntu Linux ...	None	Managed (Online)	N/A

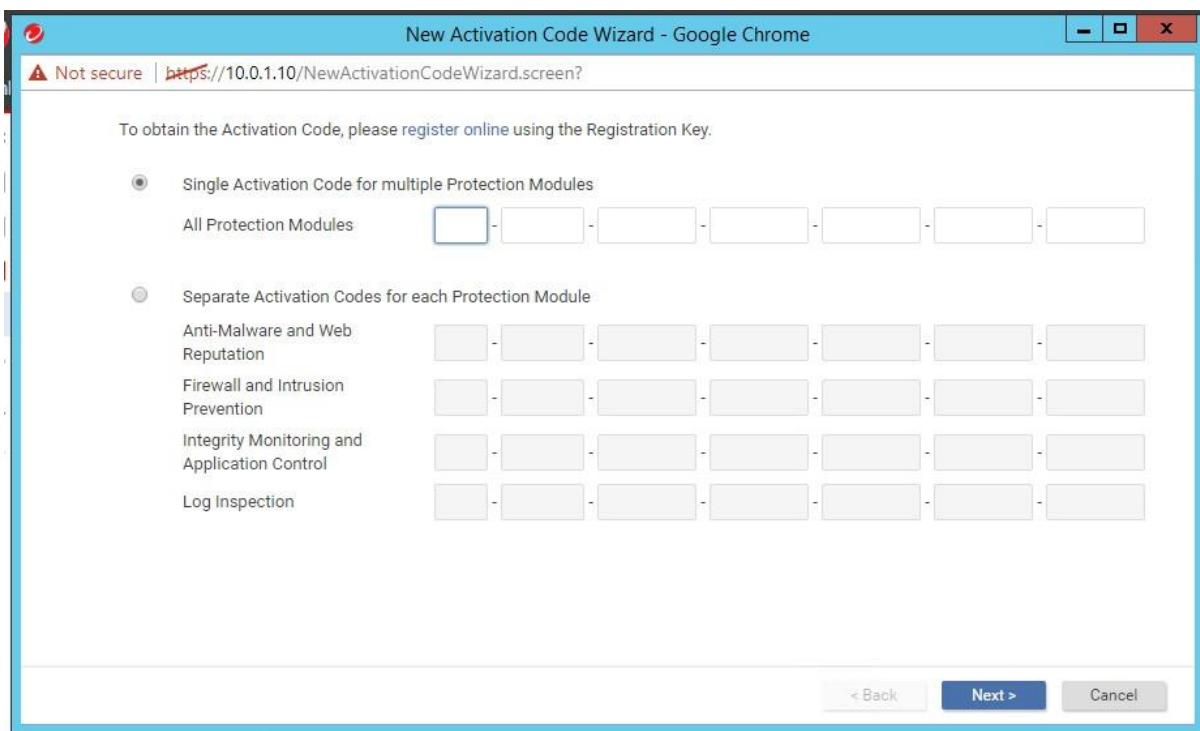
For installing the TrendMicro License, click on **Administration** from top menu.

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

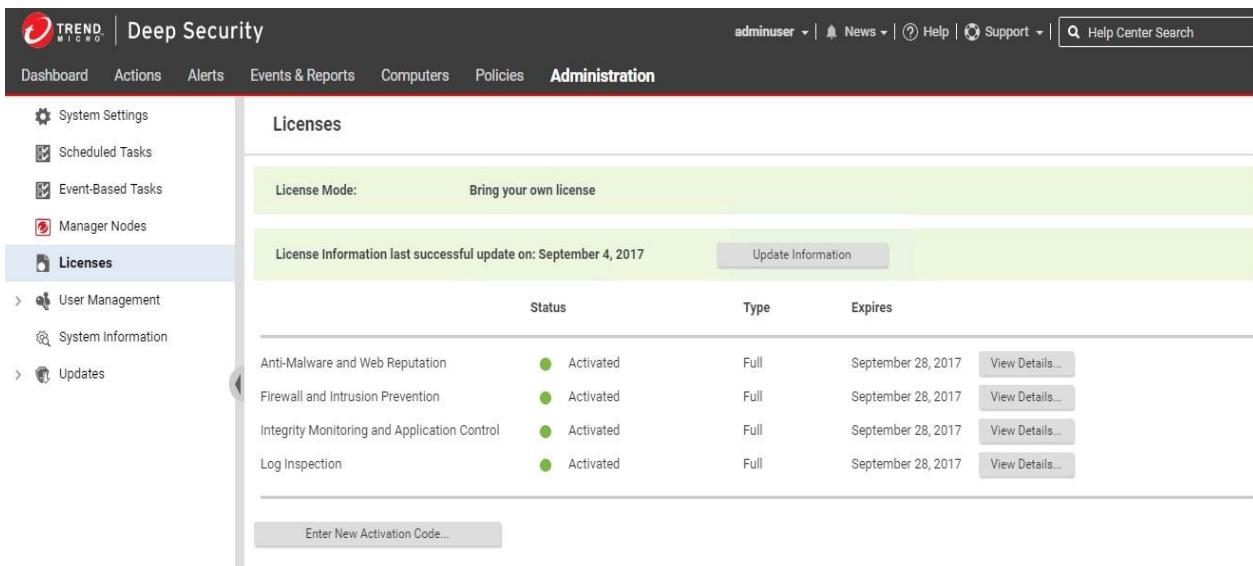
The screenshot shows the Trend Micro Deep Security interface with "Administration" selected in the top navigation. The left sidebar has "Licenses" selected (highlighted in blue). The main content area is titled "Licenses" and shows "License Mode: Bring your own license". A table lists four protection modules: Anti-Malware and Web Reputation, Firewall and Intrusion Prevention, Integrity Monitoring and Application Control, and Log Inspection. Each row shows "Not Licensed" under "Status", "N/A" under "Type", and "N/A" under "Expires". To the right of each row is a "View Details..." button. At the bottom of the table is a button labeled "Enter 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 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**



Computers		With sub-Groups	By Group	Search this page				
		Add	Delete...	Details...	Actions	Events	Export	Columns...
NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENAN...	SEND POLICY	SUCCESSFUL	
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

Overview	General	Actions	System Events
Anti-Malware	Hostname: <input type="text" value="10.0.0.6"/> (Last IP Used: 10.0.0.6)		
Web Reputation	Display Name:		
Firewall	Description:		
Intrusion Prevention	Platform:	Microsoft Windows Server 2012 R2 (64 bit) Build 9600	
Integrity Monitoring	Group:	Computers	
Log Inspection	Policy:	None	Edit
Application Control	Asset Importance:	None	Edit
Interfaces	Download Security Updates From:	Default Relay Group	Edit
Settings	Agent		
Updates	Anti-Malware	Managed (Online)	
Overrides	Web Reputation	Off, not installed, no configuration	
	Firewall	Off, not installed	
	Intrusion Prevention	Off, not installed, no rules	
	Integrity Monitoring	Off, not installed, no rules	
	Log Inspection	Off, not installed, no rules	
	Application Control	Off, not supported	
	Online	Yes	
			Save Close

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

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

Computer: 10.0.0.6

Overview	General	Smart Protection	Advanced	Identified Files	Anti-Malware Events
Anti-Malware	Configuration: Default (Off)				
Web Reputation	State: Off, not installed, no configuration				
Firewall					
Intrusion Prevention					
Integrity Monitoring					
Log Inspection					
Application Control					
Interfaces					
Settings					
Updates					
Overrides					
Real-Time Scan					
<input checked="" type="checkbox"/> Inherited					
Malware Scan Configuration:	No Configuration	Edit			
Schedule:	Select Schedule	Edit			
Manual Scan					
<input checked="" type="checkbox"/> Inherited					
Malware Scan Configuration:	No Configuration	Edit			
Scheduled Scan					
<input checked="" type="checkbox"/> Inherited					
Malware Scan Configuration:	No Configuration	Edit			
Malware scan					
Last Manual Scan for Malware:	N/A				

Save **Close**

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

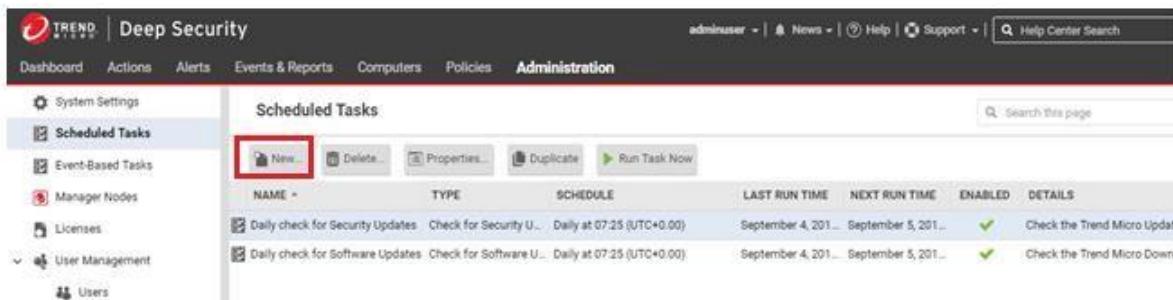
Note: it might take some time to get Activated.

Computer: 10.0.0.6

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

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

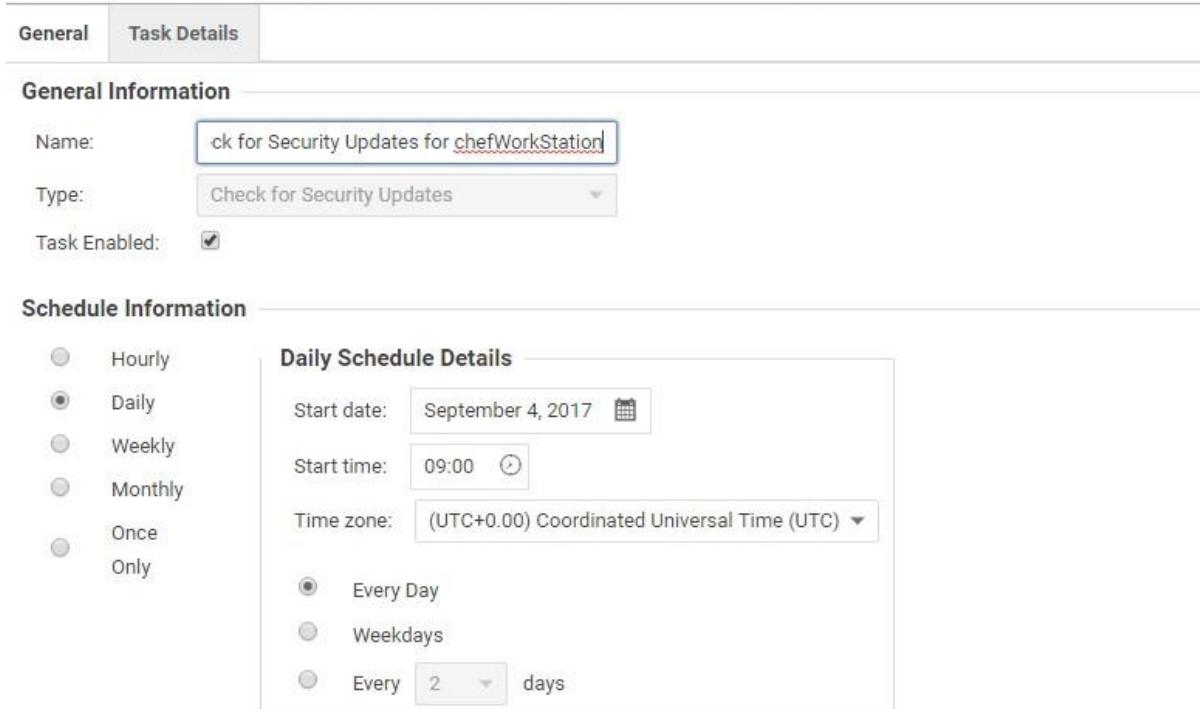
To schedule a scan, navigate to **Administration** and click on **New**.



The screenshot shows the Trend Micro Deep Security interface with the 'Administration' tab selected. Under 'Scheduled Tasks', there is a table listing two tasks: 'Daily check for Security Updates' and 'Daily check for Software Updates'. Both tasks are set to run daily at 07:25 UTC+0.00. The 'New...' button is highlighted with a red box.

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

 Not secure | <https://10.0.1.10/ScheduledTaskProperties.screen?scheduledTaskID=3>



The screenshot shows the 'Scheduled Task Properties' screen with the 'General' tab selected. In the 'General Information' section, the 'Name' field contains 'Check for Security Updates for chefWorkStation'. The 'Type' dropdown is set to 'Check for Security Updates'. The 'Task Enabled' checkbox is checked. In the 'Schedule Information' section, the 'Daily' radio button is selected. The 'Start date' is set to 'September 4, 2017' and the 'Start time' is '09:00'. The 'Time zone' is '(UTC+0.00) Coordinated Universal Time (UTC)'. Below these, there are three options: 'Every Day' (selected), 'Weekdays', and 'Every 2 days'.

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

New Scheduled Task Wizard - Google Chrome

⚠ Not secure | <http://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:	<input type="text" value="Daily Check for Security Updates for chefWorkStation"/>
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.



TREND MICRO | 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,
Daily check for Security Updates	Check for Security U...	Daily at 07:25 (UTC+0:00)	September 4, 201...	September 5,
Daily check for Software Updates	Check for Software U...	Daily at 07:25 (UTC+0:00)	September 4, 201...	September 5,

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

TREND MICRO | 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

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
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

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

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	Info	2204	Select All (14)	Agent	10.0
September 4, 2017 08:59:59	Info	273	Export Selected to CSV...	Manager	10.0
September 4, 2017 08:59:59	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0
September 4, 2017 08:59:59	Info	710	Events Retrieved	Agent	10.0
September 4, 2017 08:59:59	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0
September 4, 2017 08:59:59	Info	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

Actions

System Events

TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGIN	TARGET
September 4, 2017 09:03:52	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 09:00:25	Info	Select All (14)	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:25:42	Info	Export Selected to CSV...	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:20:24	Info	View	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:15:32	Info	Add Tag(s)...	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:15:32	Info	Remove Tag(s)...	Events Retrieved	Agent	10.0	
September 4, 2017 08:15:32	Info	...	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

Quick access

- Desktop
- Downloads

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

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

Clipboard

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 Agent	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.

TREND MICRO | Deep Security

adminuser | News | Help | Support | Help Center Search

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

Alerts Summary View By Time

Computers: All Computers

Recommendations have been made for 1 Computer(s)

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.)

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)

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

August 31, 2017 12:43

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

TREND MICRO | Deep Security

adminuser | News | Help | Support | Help Center Search

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

Alerts List View No Grouping

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 ...	10.0.1.11	
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

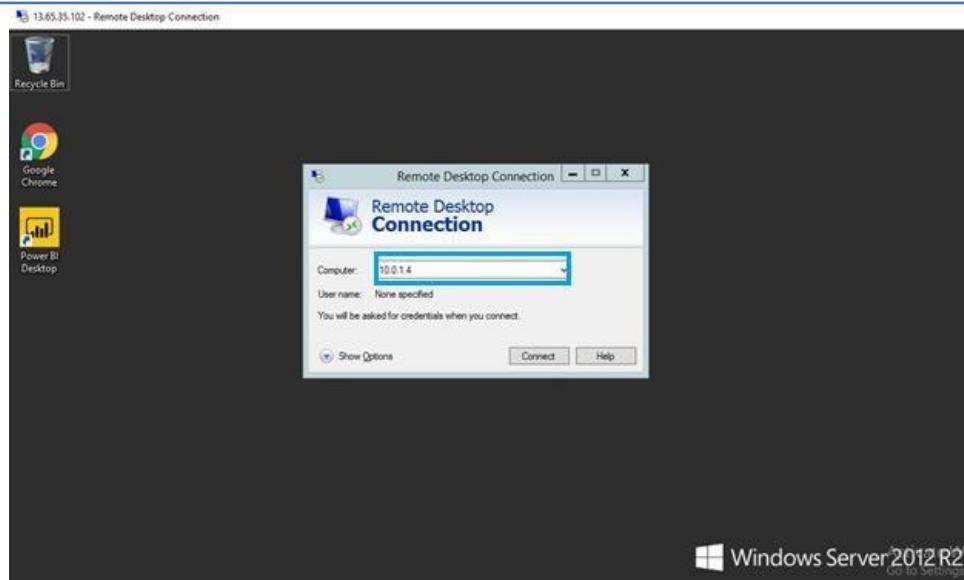
8. Create User for PI Business Analytics (PIBA) Interface

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

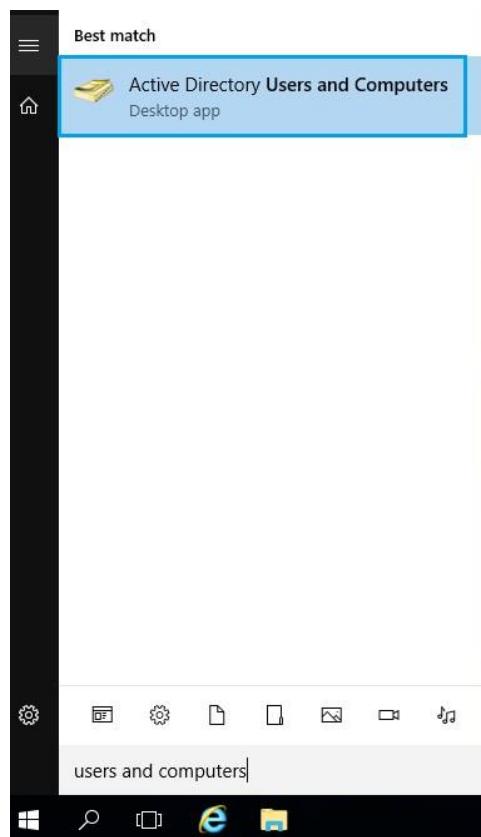
Outputs	
ADMINUSERNAME	adminuser
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com
ADSERVERIPADDRESS	10.0.1.4



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**.

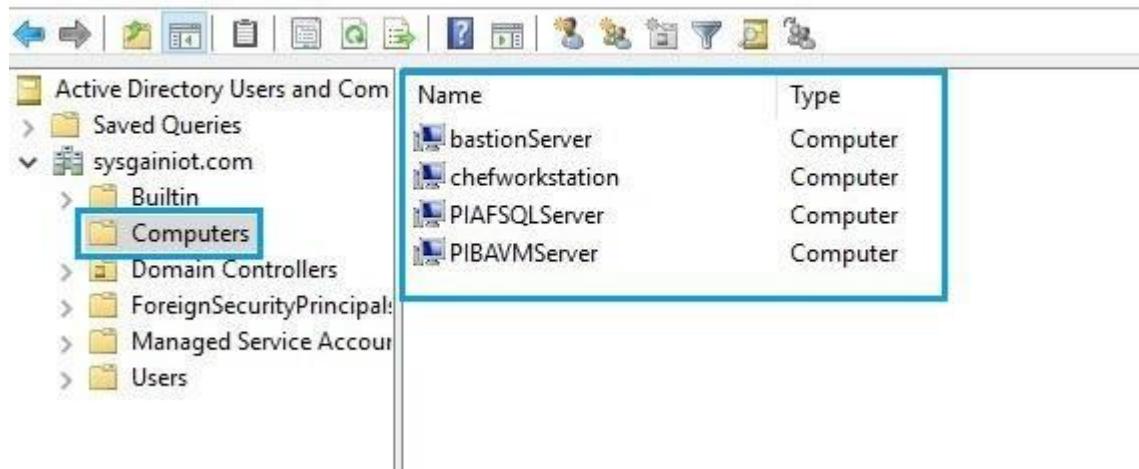


4. Click on domain name which you created. Select **Computers** to see the list of virtual machines added to the active directory. The following Virtual Machines that are added into the Active Directory are:

- Bastion server
- Chef workstation
- PIAF SQL Server
- PIBA VM Server
- PIDA VM Server

Active Directory Users and Computers

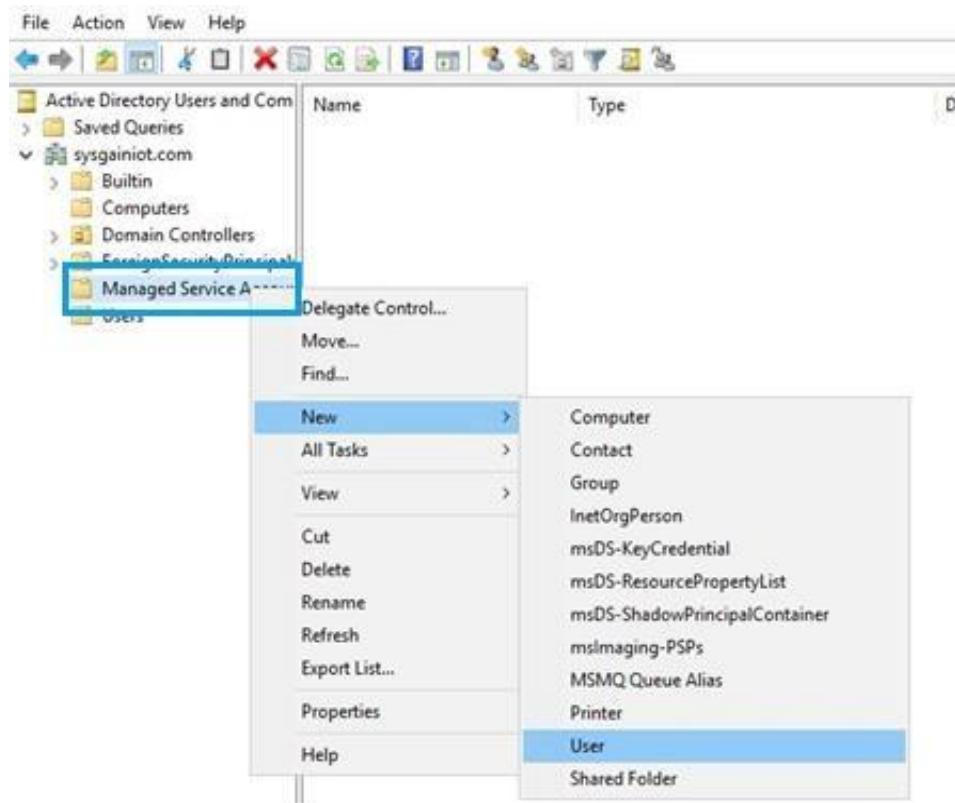
File Action View Help



The screenshot shows the Windows Active Directory Users and Computers snap-in. The left pane displays a tree view of the directory structure. Under the 'sysgainiot.com' domain, the 'Computers' folder is selected and highlighted with a blue border. The right pane shows a table of computer objects:

Name	Type
bastionServer	Computer
chefworkstation	Computer
PIAFSQLServer	Computer
PIBAVMServer	Computer

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

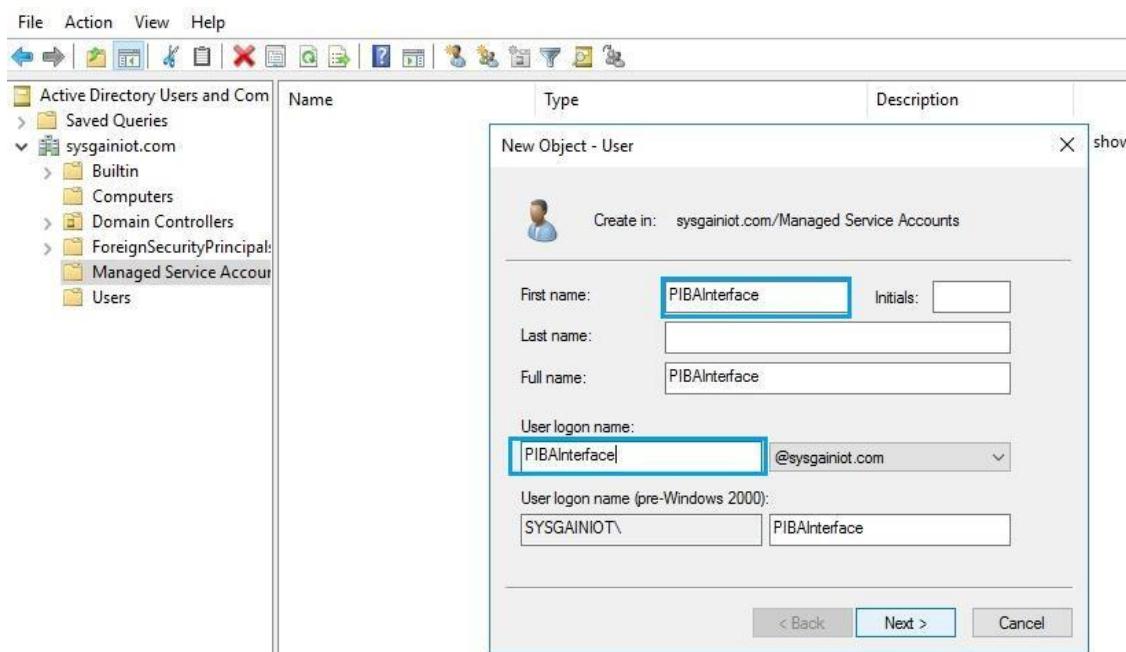


The screenshot shows the same Active Directory interface. A context menu is open over a 'Managed Service Account' object. The 'New' option in the menu is expanded, showing various object types. The 'User' option is highlighted with a blue selection bar.

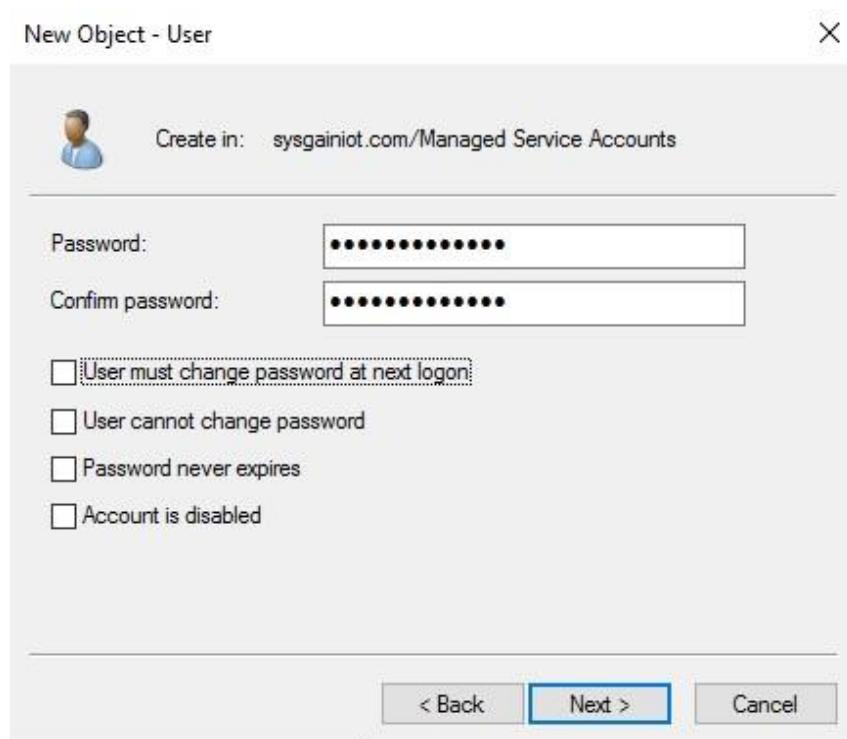
- Delegate Control...
- Move...
- Find...
- New** >
- All Tasks >
- View >
- Cut
- Delete
- Rename
- Refresh
- Export List...
- Properties
- Help

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

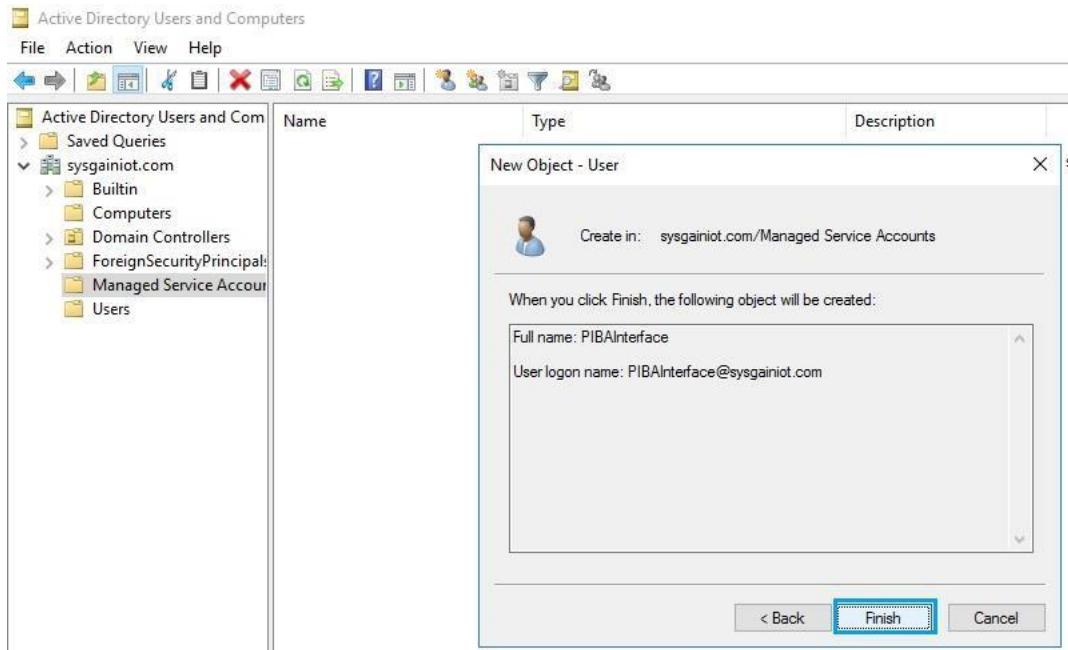
6. To create the user for PIBA, enter the **First name** and **User logon name** as **PIBAInterface**. Make sure both are same. Click on **Next**.



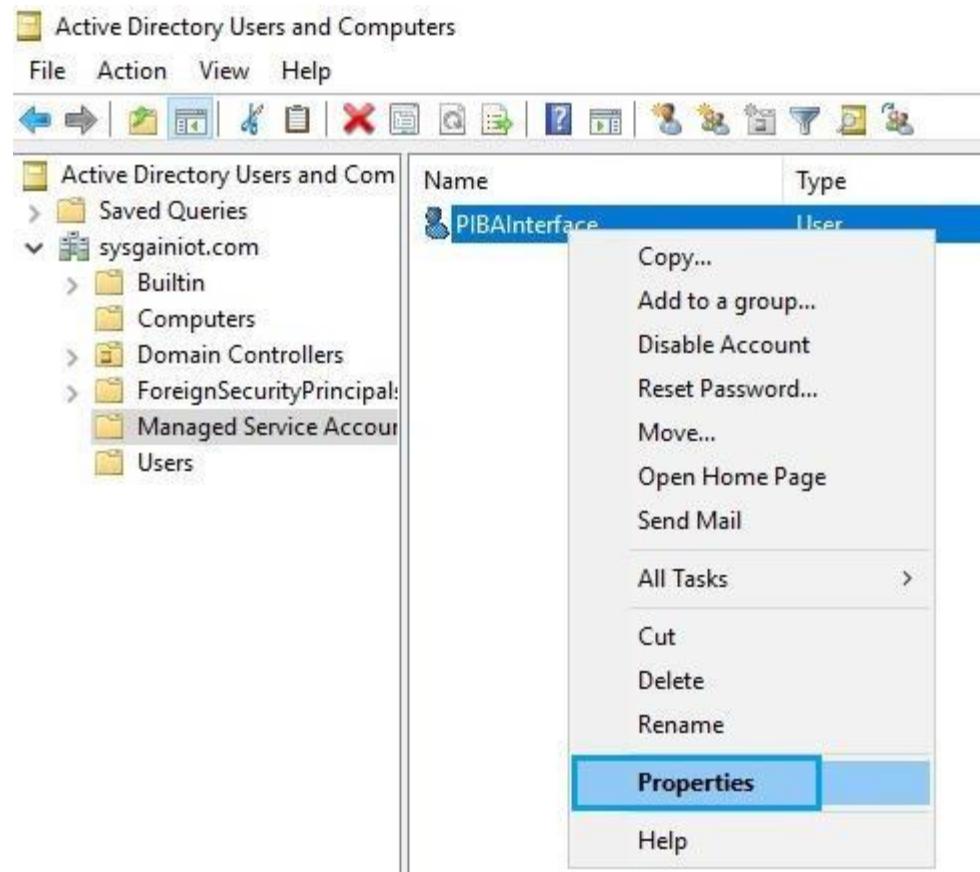
7. Enter the **Password** and uncheck **User must change password at next logon**. Click on **Next**.



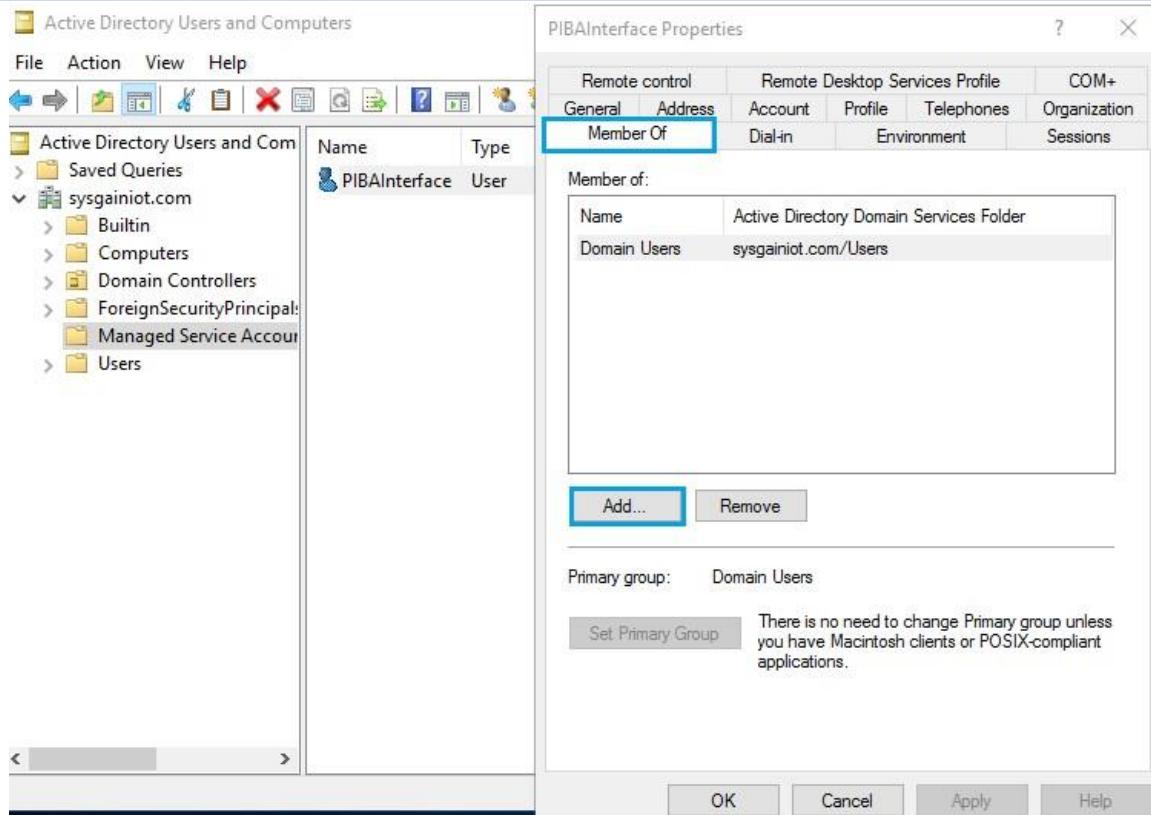
8. Click **Finish** once the object is created.



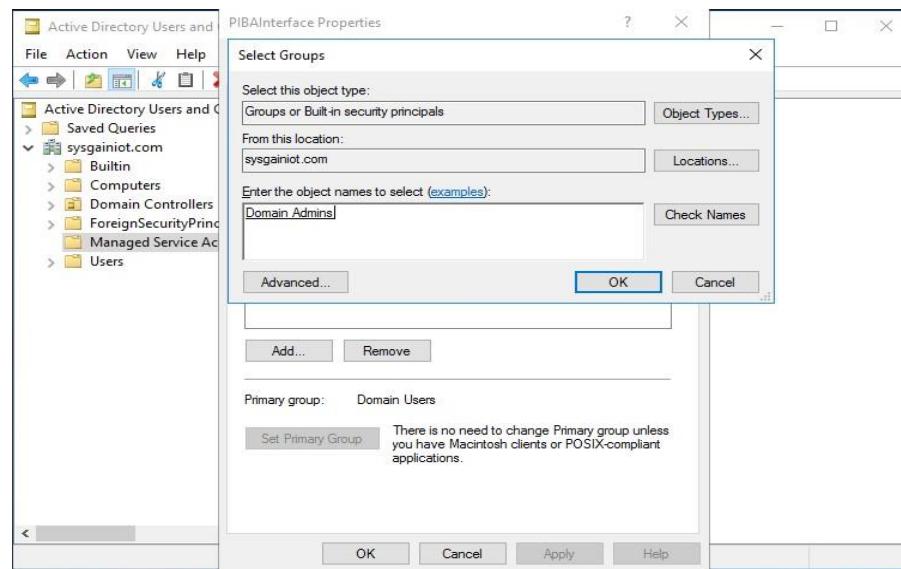
9. Check on the properties of the user created. Right click on the **PIBAInterface** and click on **Properties**.



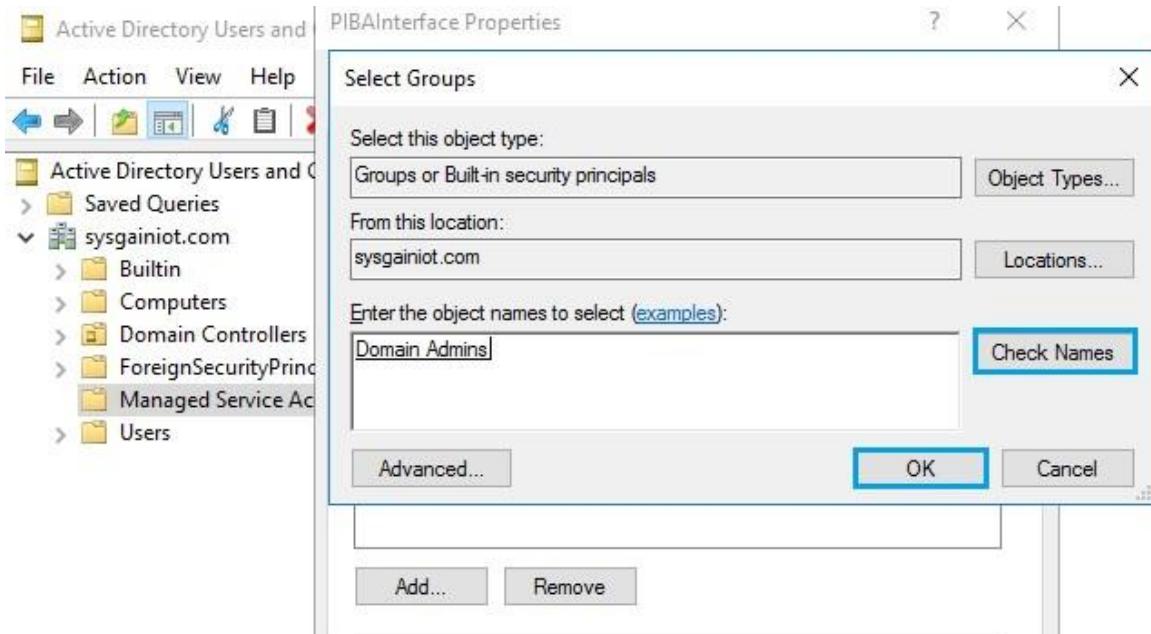
10. A popup will appear. Click on the **Member Of** tab and click the **Add** button.



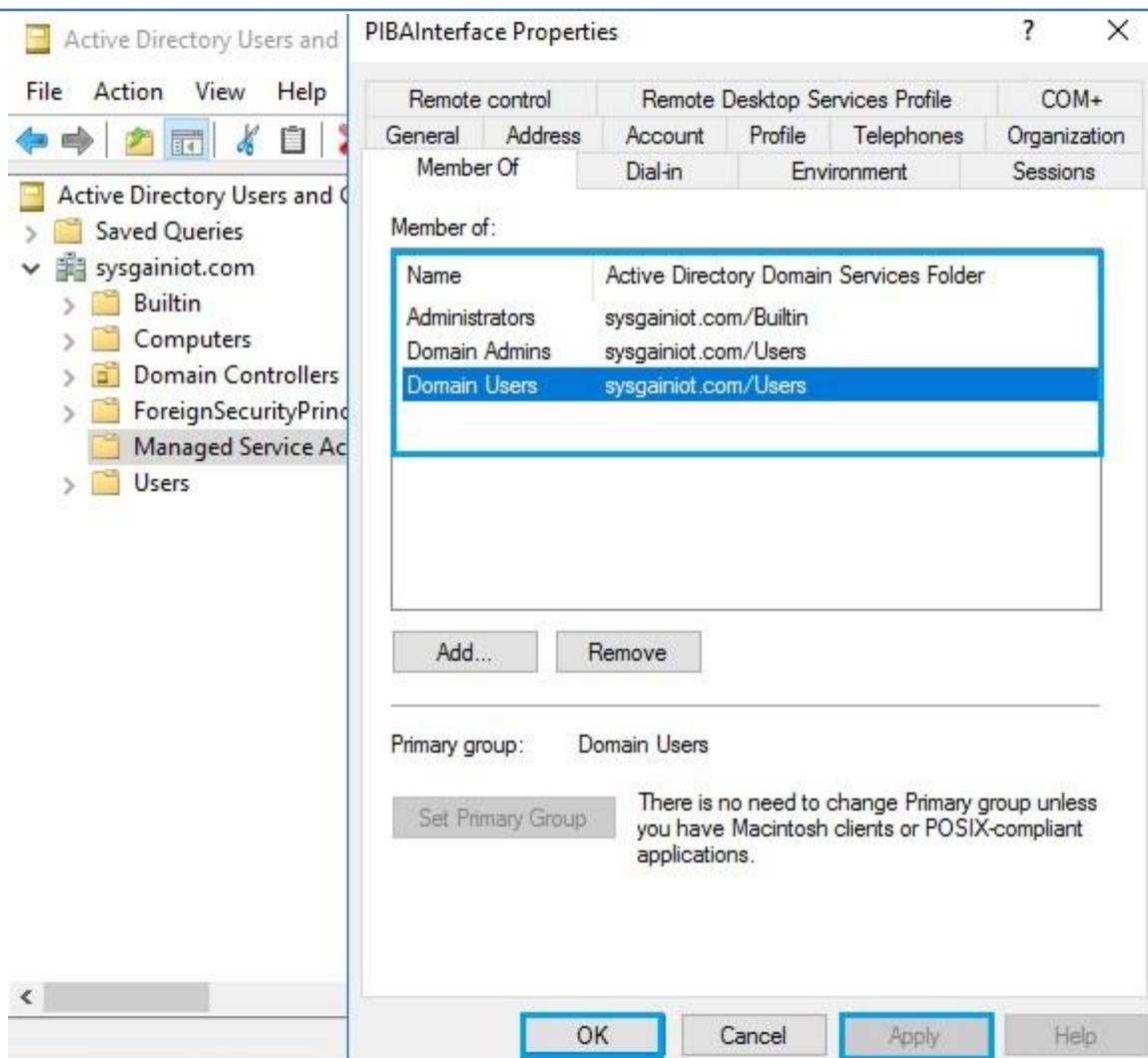
11. Enter the object name as **Domain Admins** and click on **Check Names**. It will display the Domain Admins as object names. Click on **Ok**. After that, click on **Ok** again. You will see the Domain Admin name added to the **Member of** section.



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



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



8.1. Create PIBA User in PIAF Server

- 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	



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

Connect to Server X

SQL Server

Server type: Database Engine

Server name: PIAFSQLServer

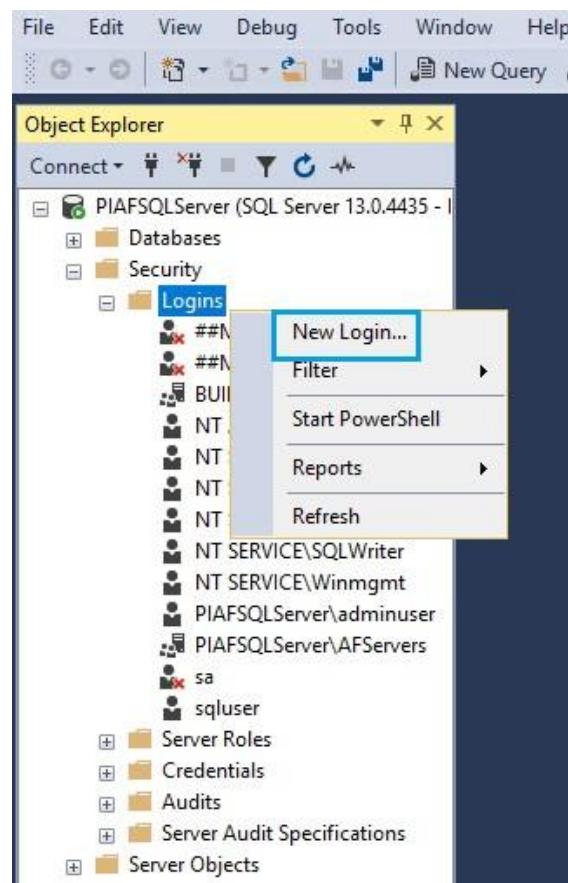
Authentication: Windows Authentication

User name: PIAFSQLServer\adminuser

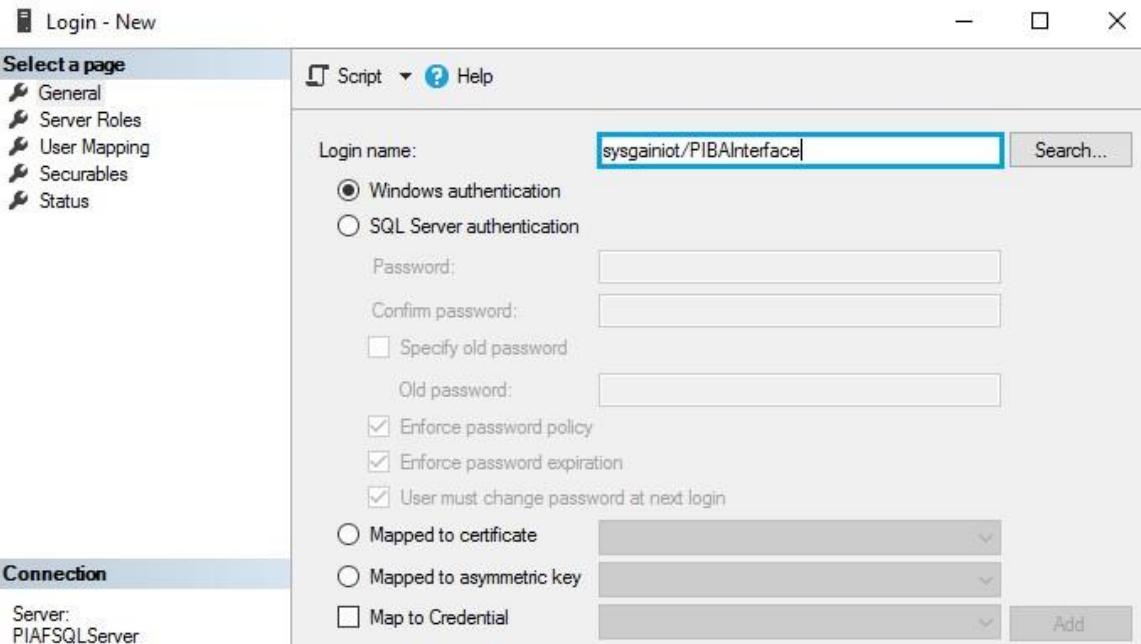
Password:

Remember password

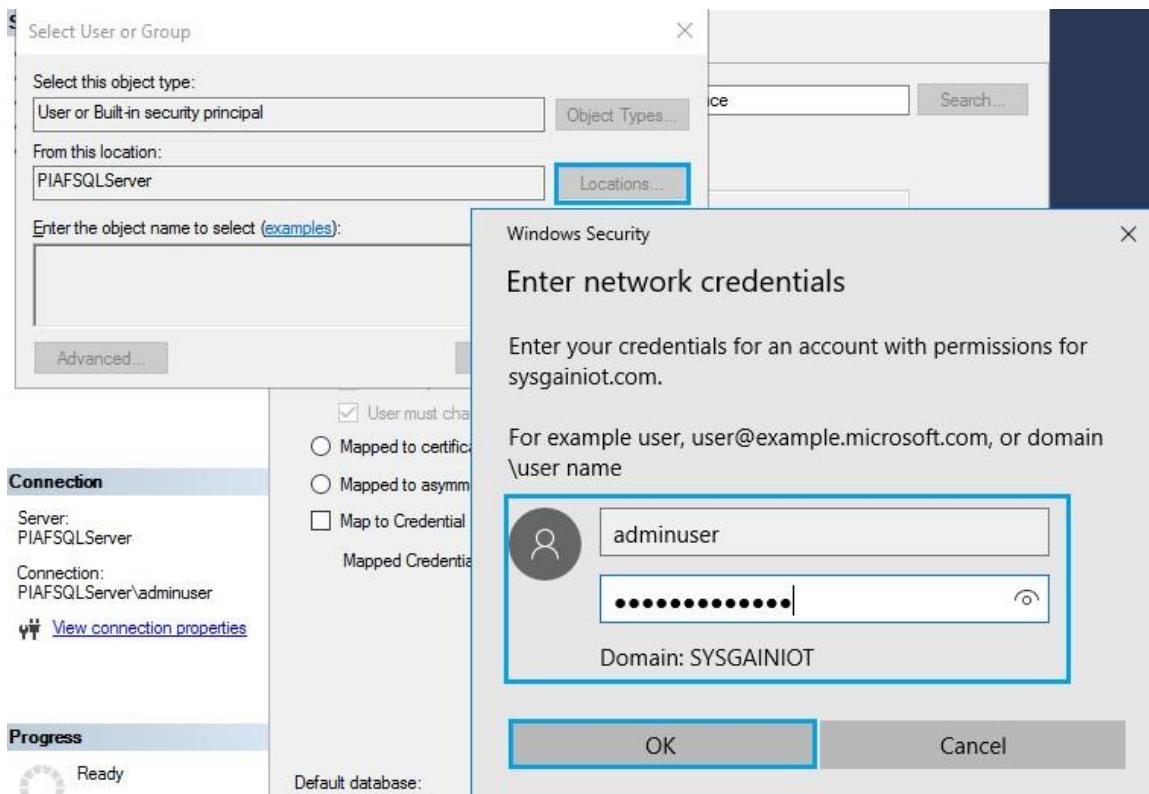
Connect Cancel Help Options >>



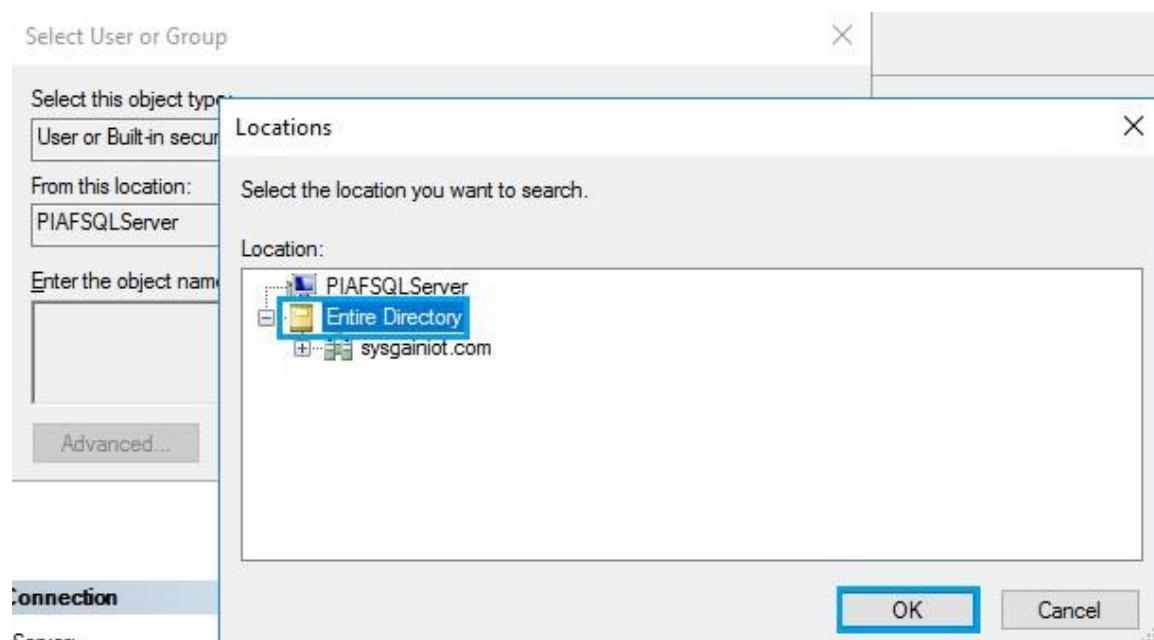
3. Give the login name as **domain name** without .com/**PIBAInterface**, then click on **Search**.



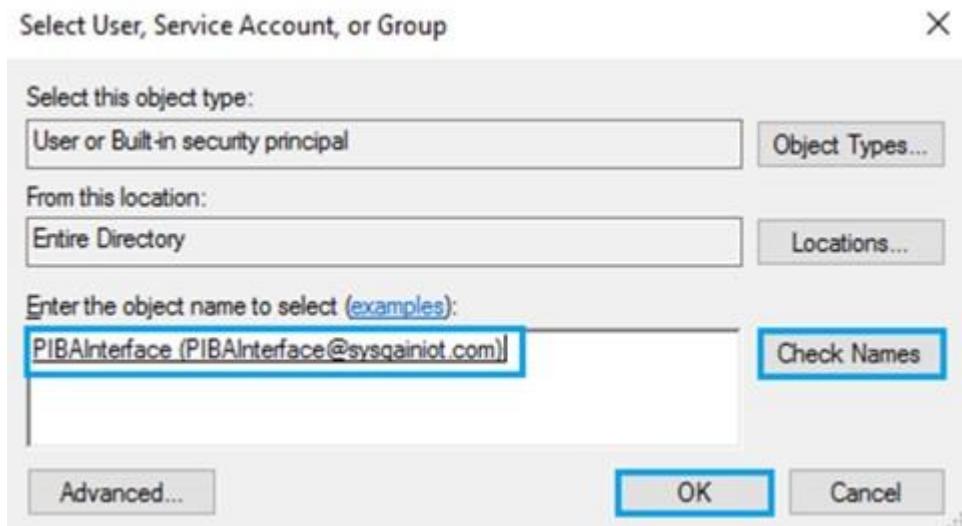
4. Click on **Locations**. You will get a popup box of credentials: enter the SQL server credentials.



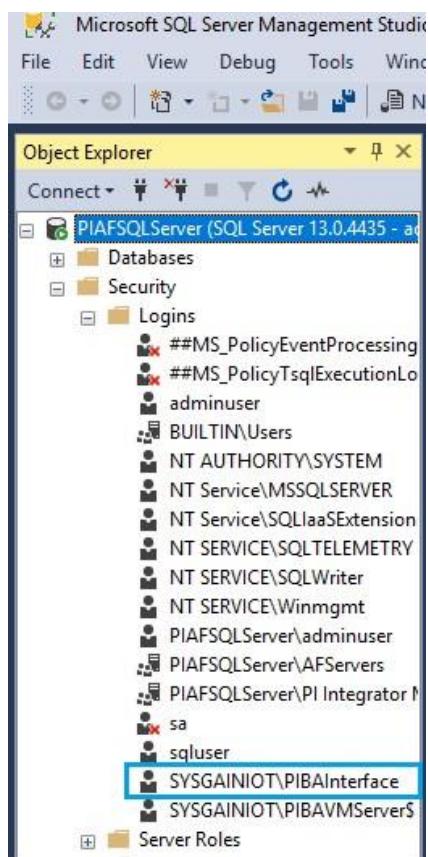
5. Select the **Entire Directory** and click on **OK**.



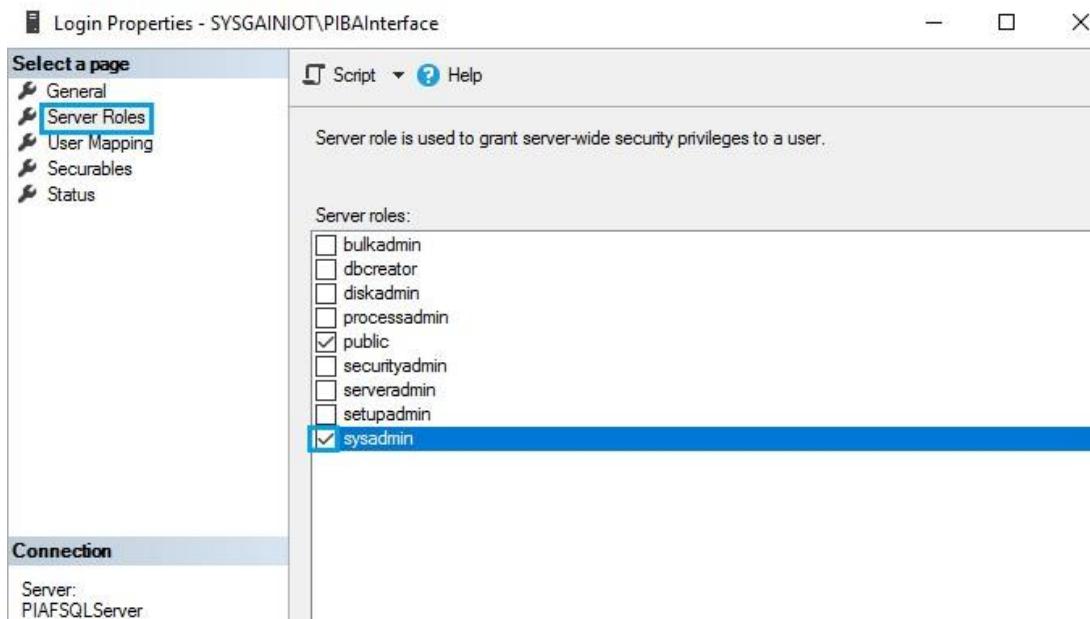
6. Enter the object name as **PIBAInterface** and click on **Check Names**. Then click on **OK**



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

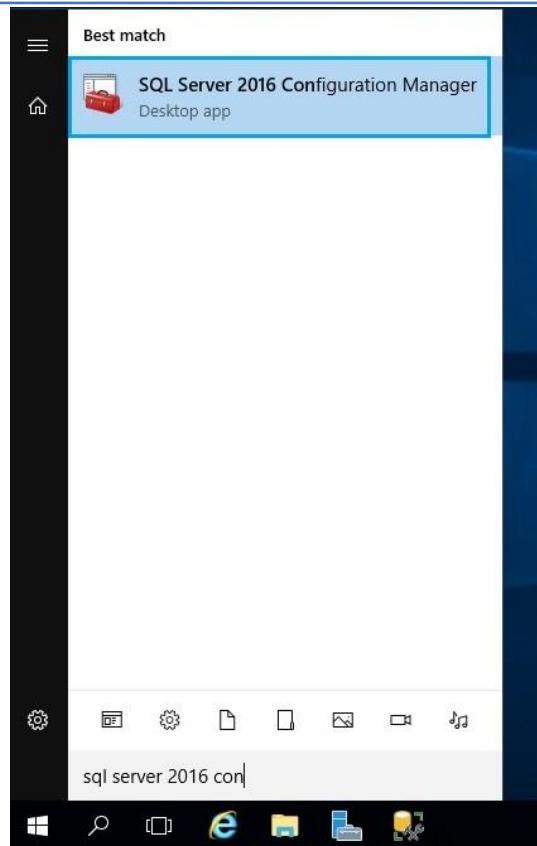


8. Right click on **User (created)** > Right click and select **properties** > click **Server Roles** > check the **sysadmin** box to give permission to the new user.

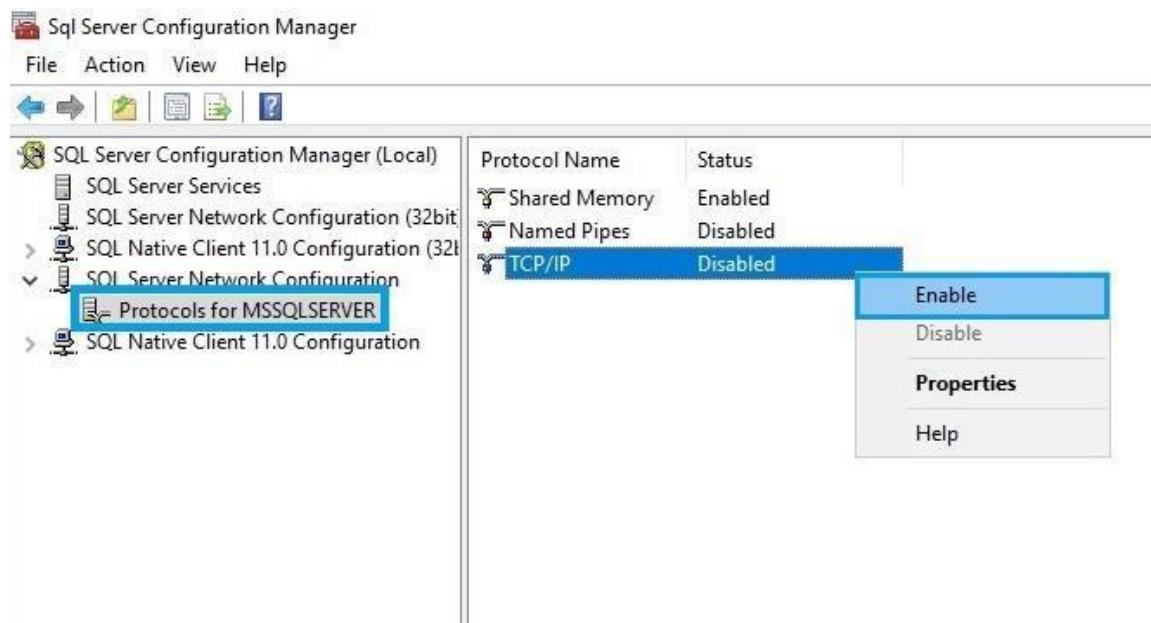


8.2. Enable TCP and Named Pipe in SQL Server Configuration Management

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



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

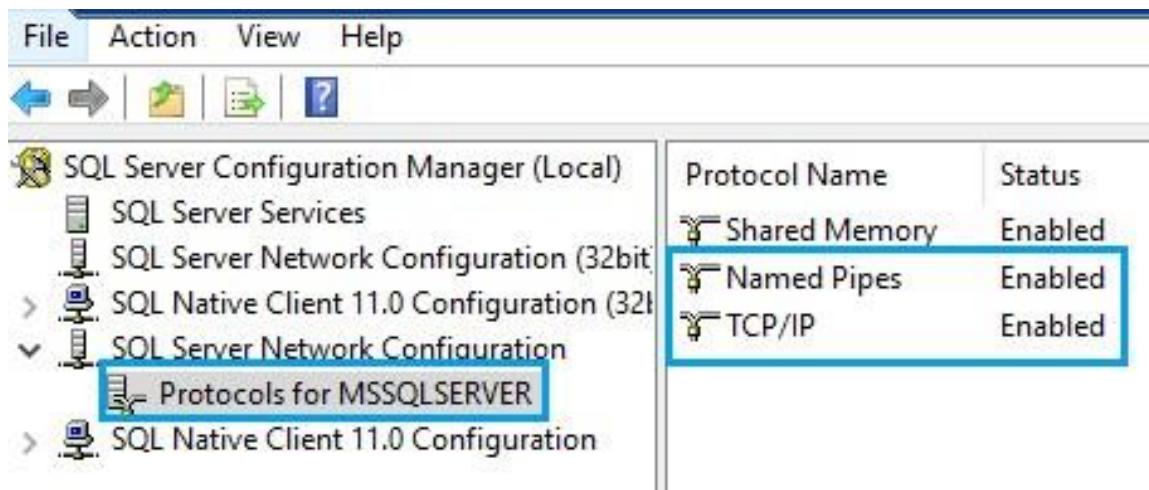


The screenshot shows the SQL Server Configuration Manager interface. On the left, the tree view is expanded to show 'Protocols for MSSQLSERVER' under 'SQL Server Network Configuration (32bit)'. In the main pane, there is a table with two rows:

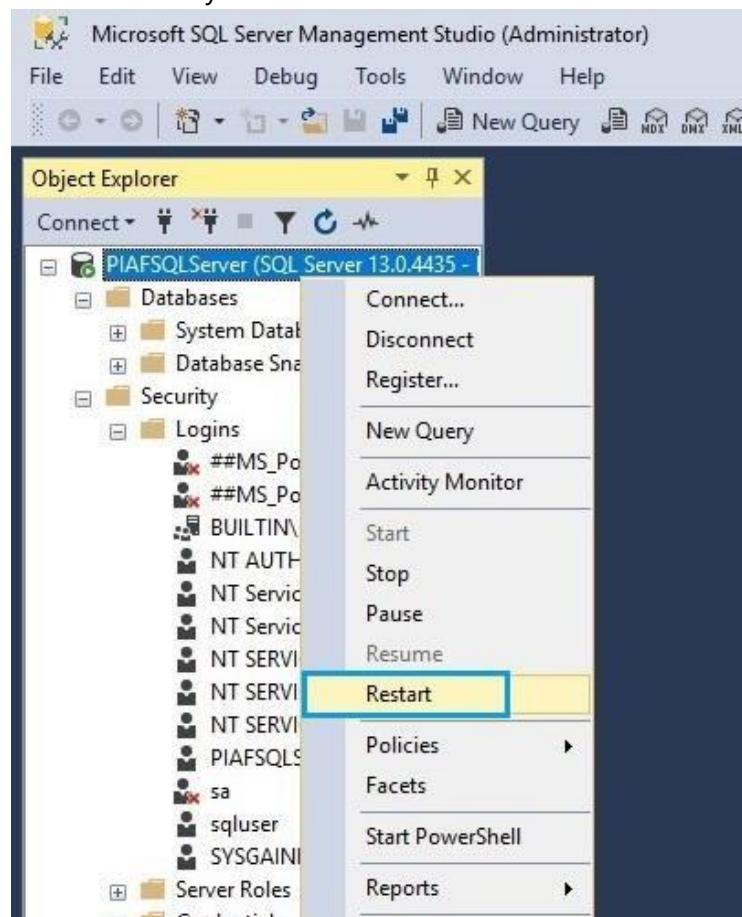
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Disabled

A context menu is open over the 'TCP/IP' row, with the 'Enable' option highlighted. The menu also includes 'Disable', 'Properties', and 'Help' options.

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



- 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

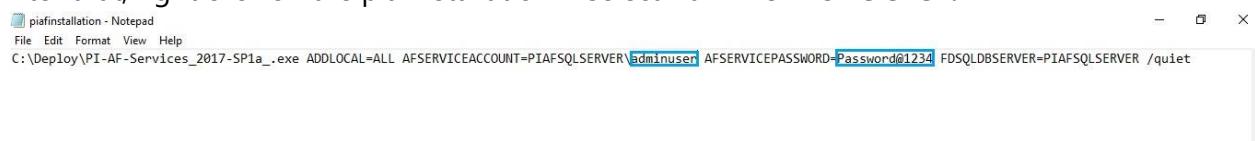
10.0.1.4

PIAFSQLSERVERIPADDRESS

10.0.2.4



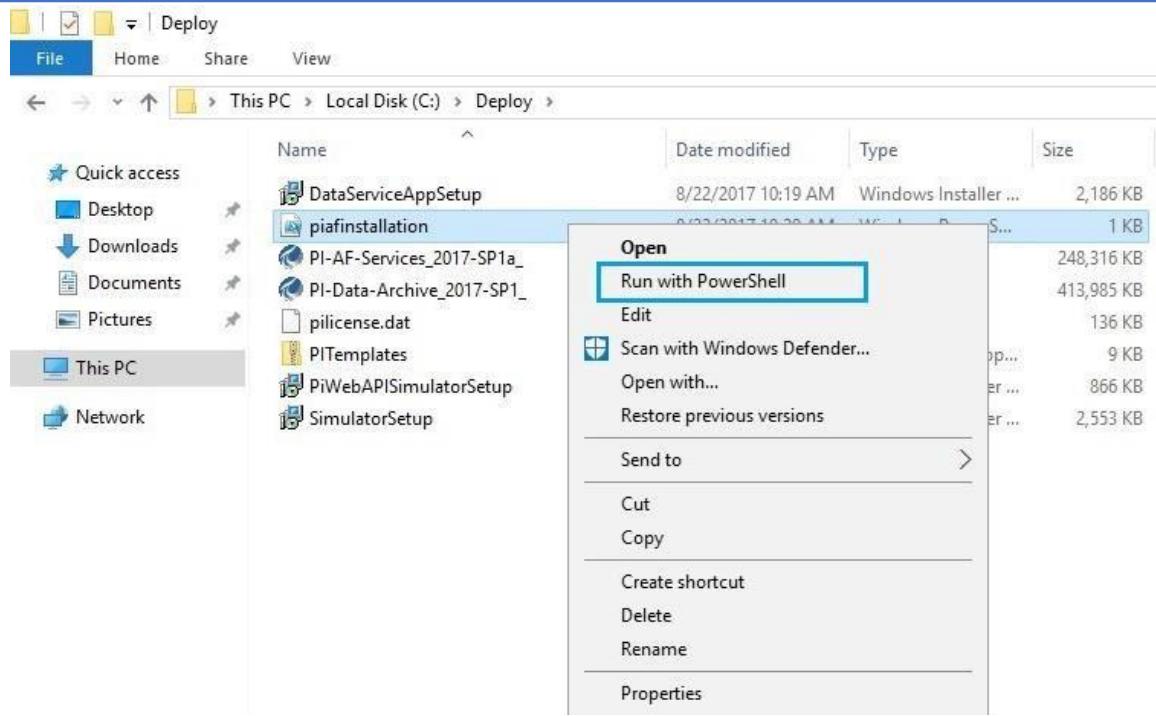
2. Navigate to **Local disk (C:) > Deploy** > Right click on **piafinstallation** > Open with Notepad. In the PowerShell script, edit the **adminuser** and **Password@1234** values to update them with your username and password from the PIAFSQLServer and then **save**. After that, right click on the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



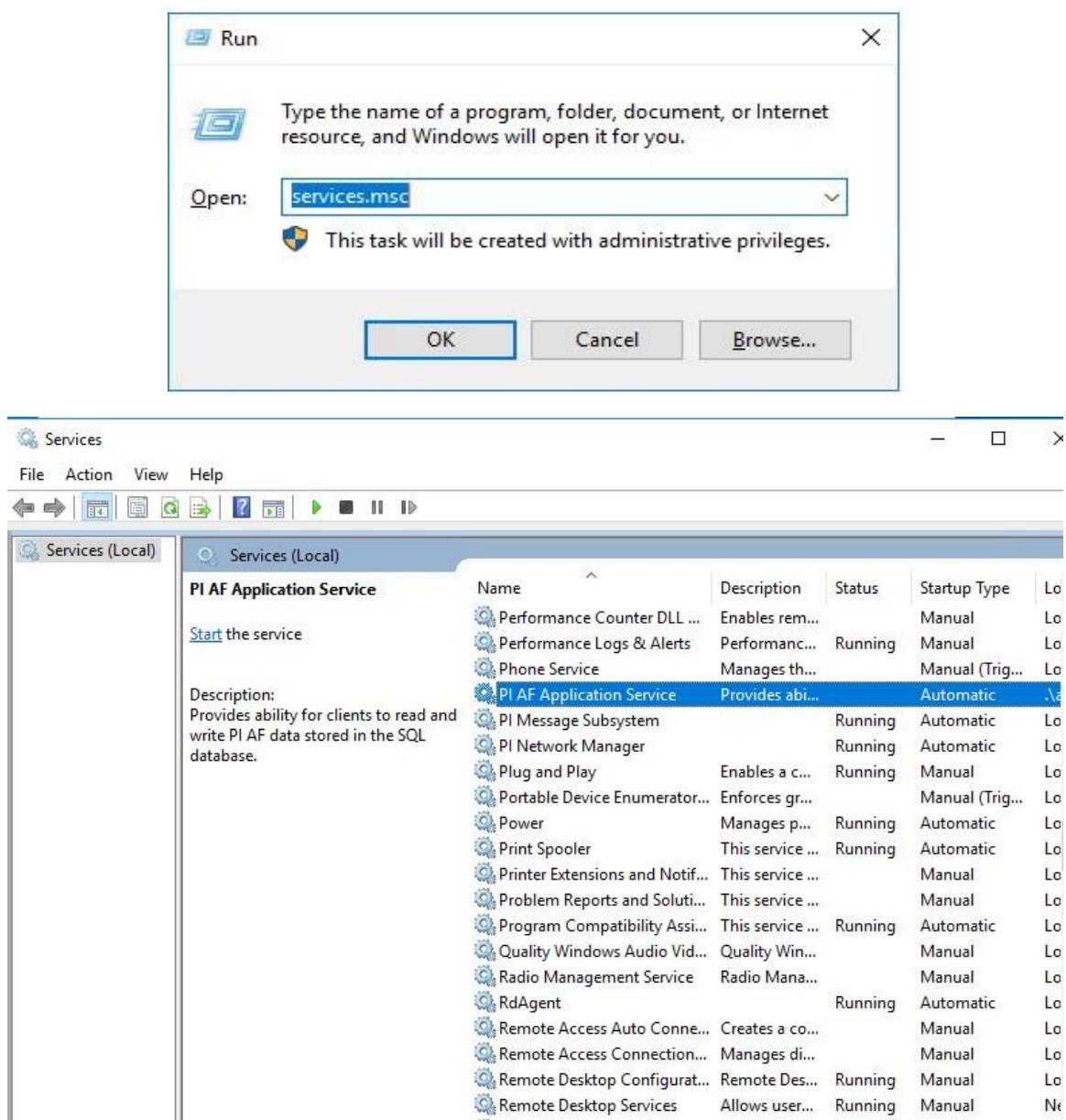
```

piafinstallation - Notepad
File Edit Format View Help
C:\Deploy\PI-AF-Services_2017-SP1a_.exe ADDLOCAL=ALL AFSERVICEACCOUNT=PIAFSQLSERVER\adminuser 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").



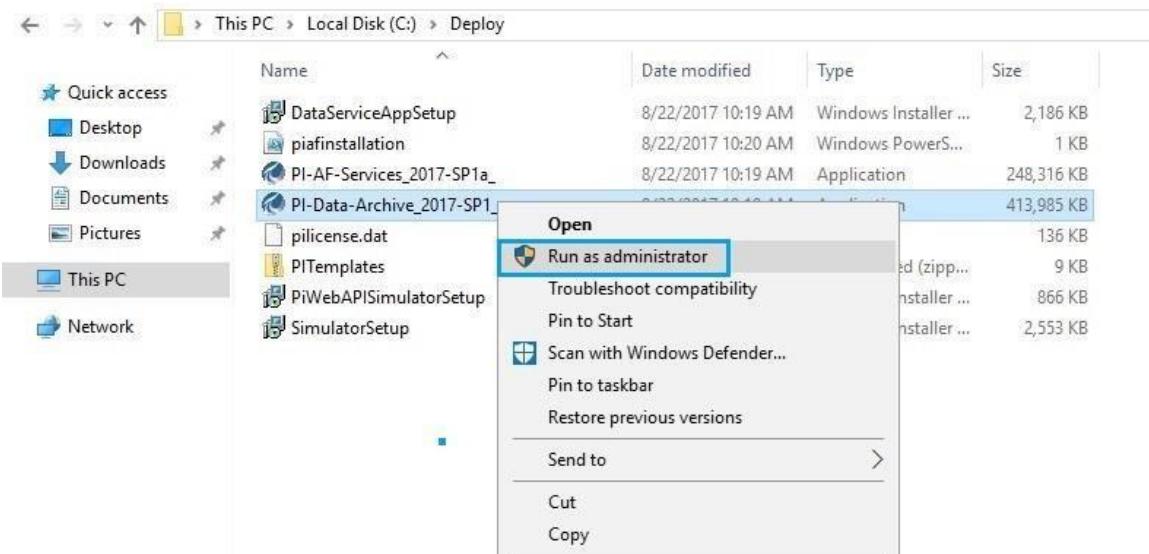
9.2. PI Data Archive (PIDA)

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.

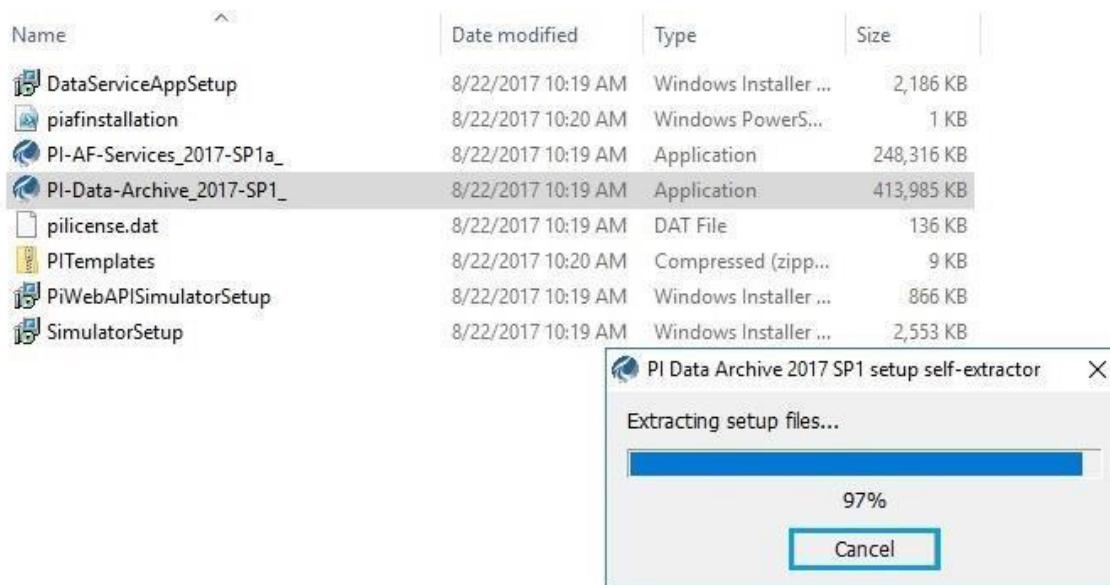
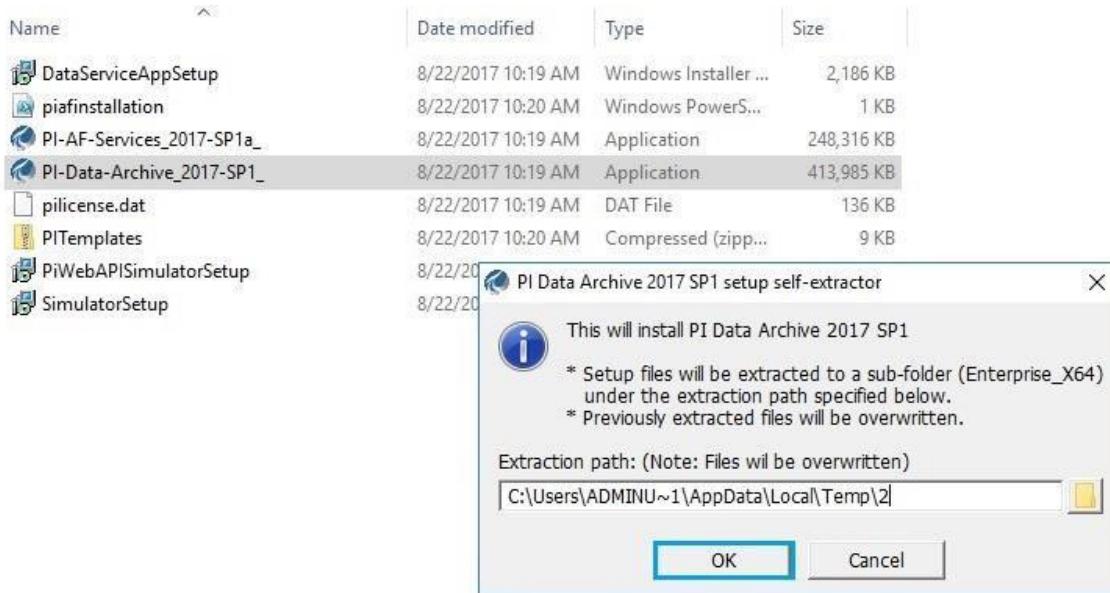
The PI Data Archive collects, stores, and organizes data from data sources, providing an information infrastructure. The PI Server also includes tools for analytics, alerts, and auditing. The PI Server may be connected to almost any existing automation, lab, or information system. Operators, engineers,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

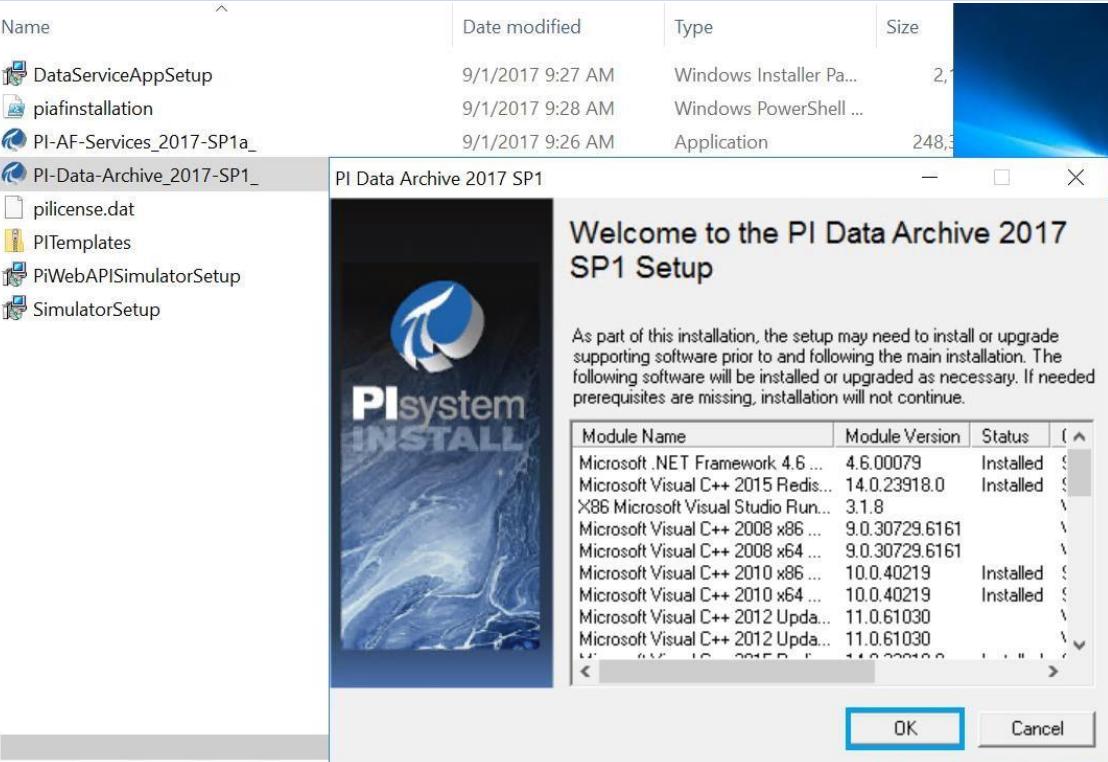
1. Navigate to **Local disk (C:) > Deploy** > select **PI-Data-archive_2017-SP1** > right click and **Run as administrator**.



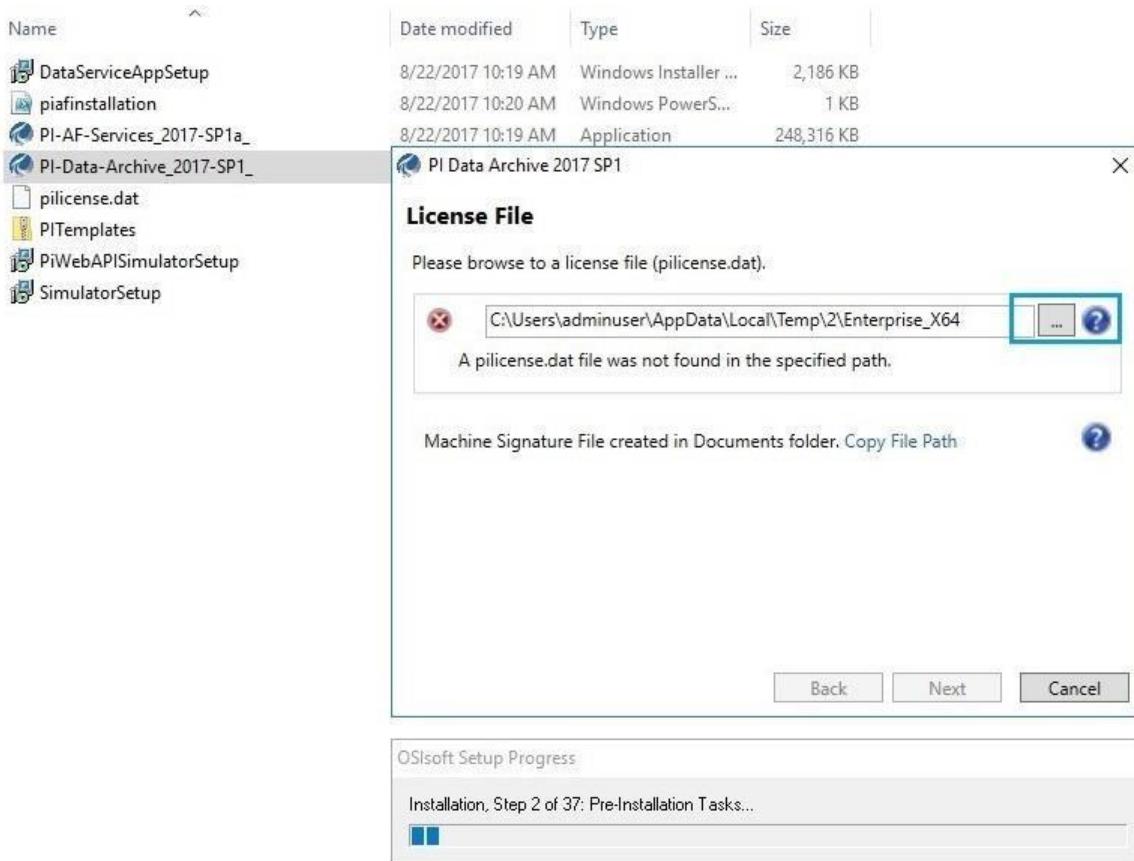
2. Click on **OK**.



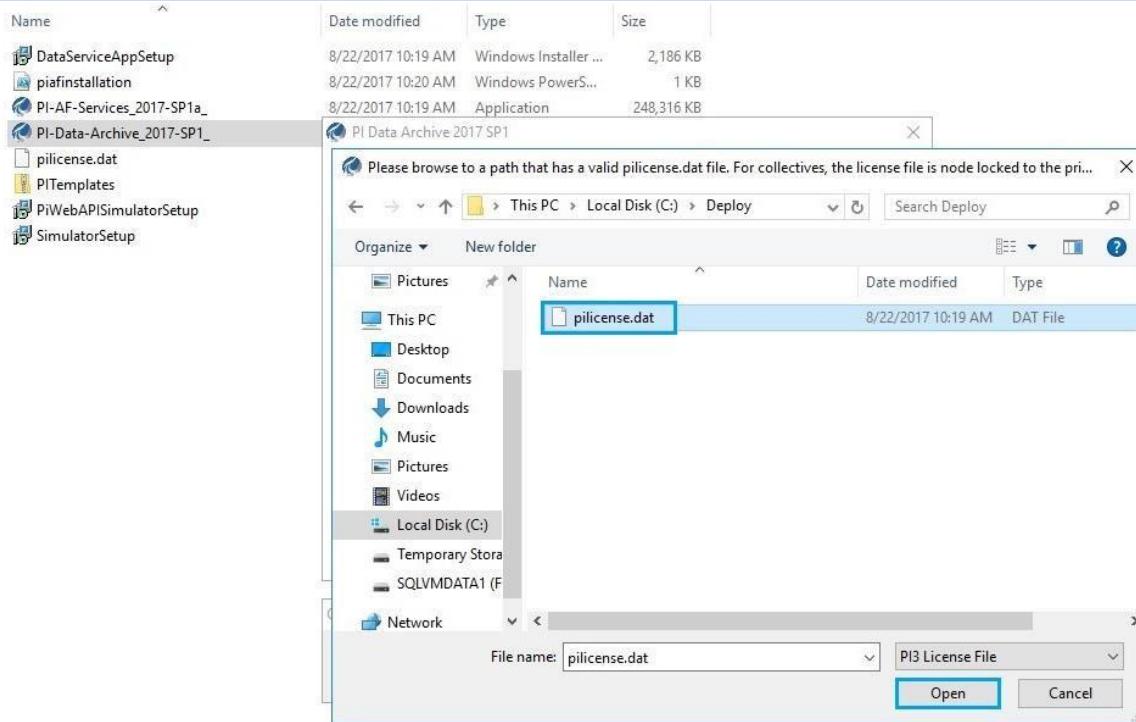
- Click on **OK**.



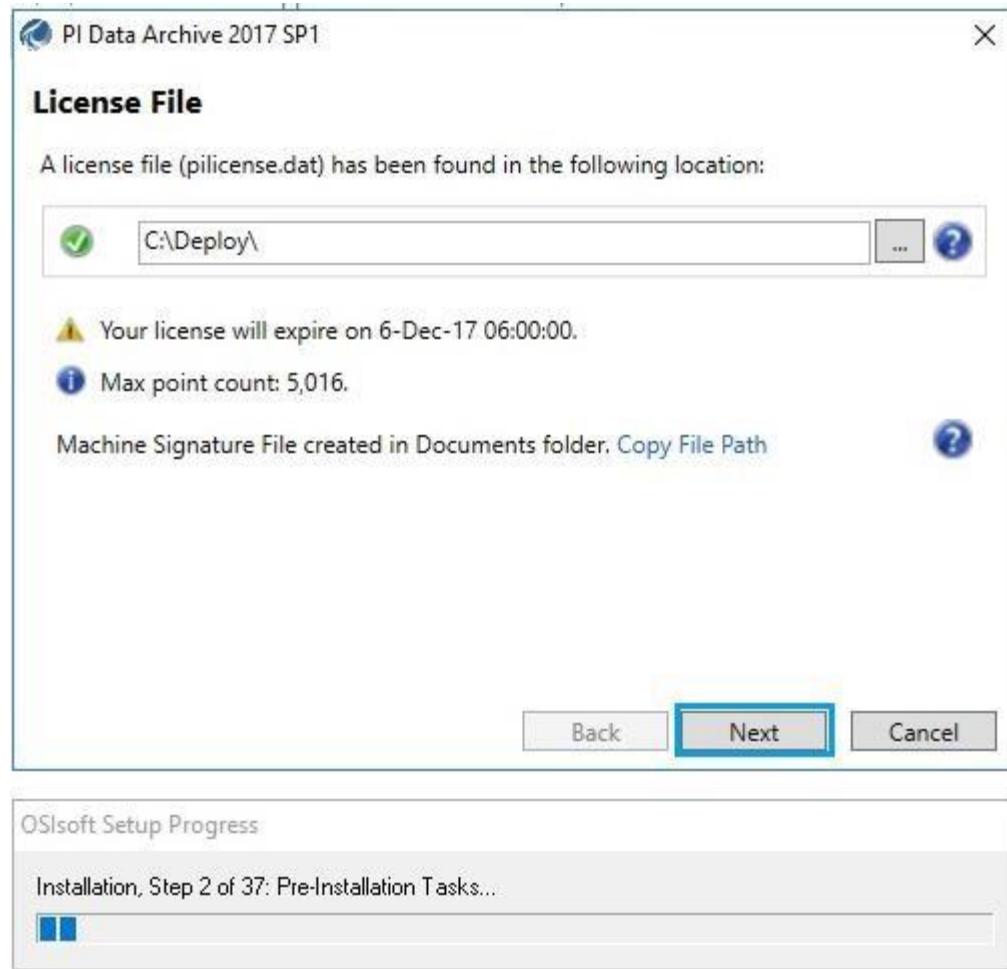
- After completion of extracting setup files, click on **OK**.



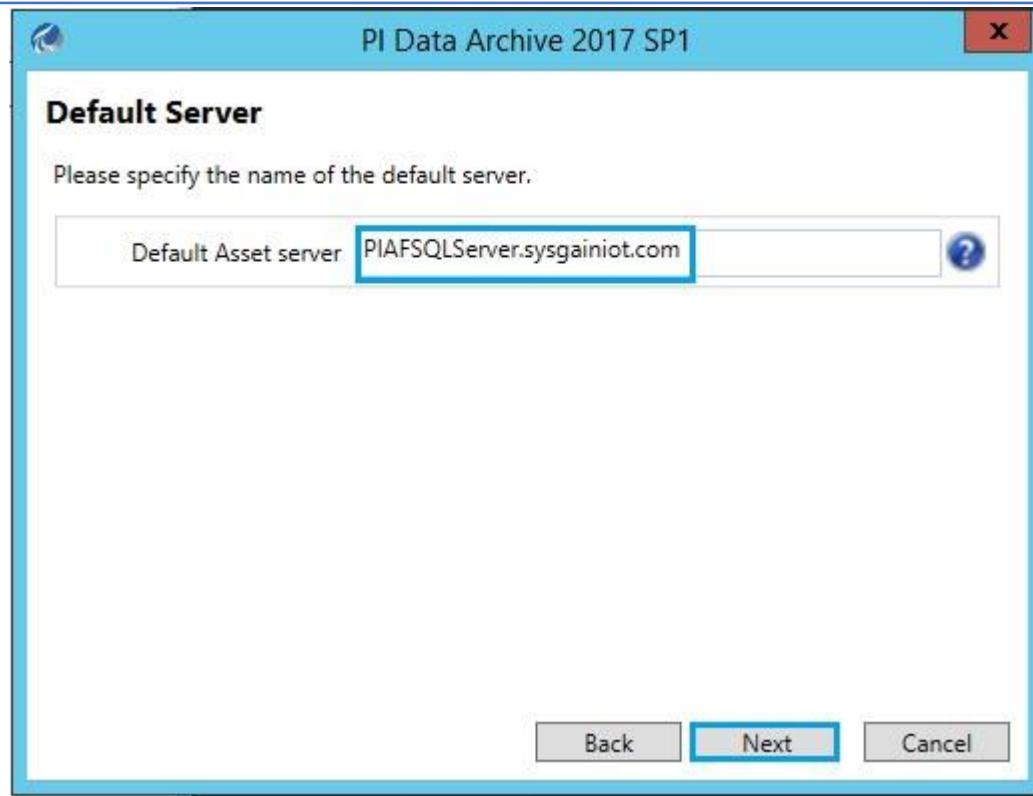
5. Click on the browse option, then navigate to the **Local disk (C:)** > **Deploy** > select **pilicense.dat** and click on **Open**.



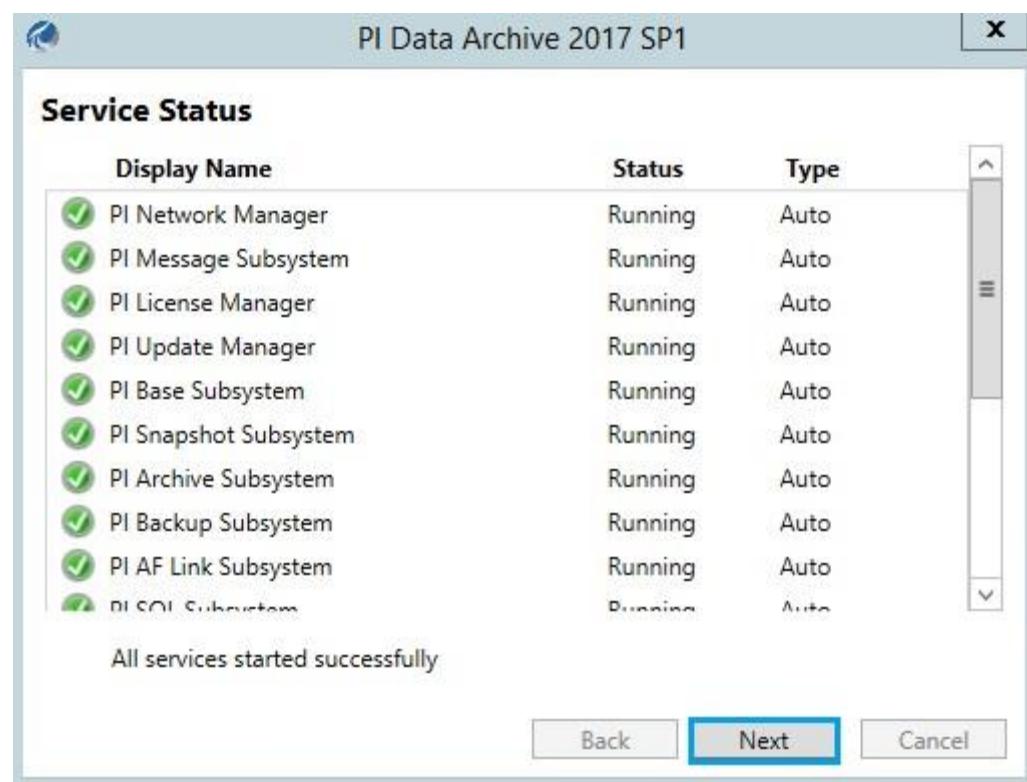
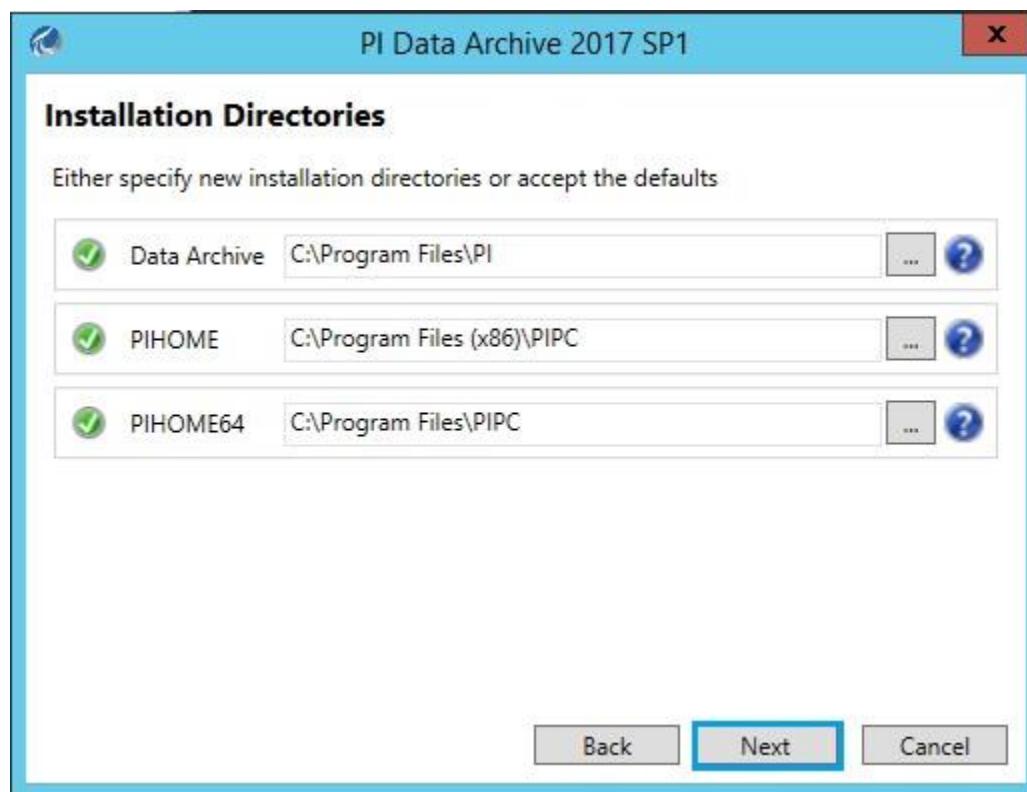
6. After that, click on **Next**.



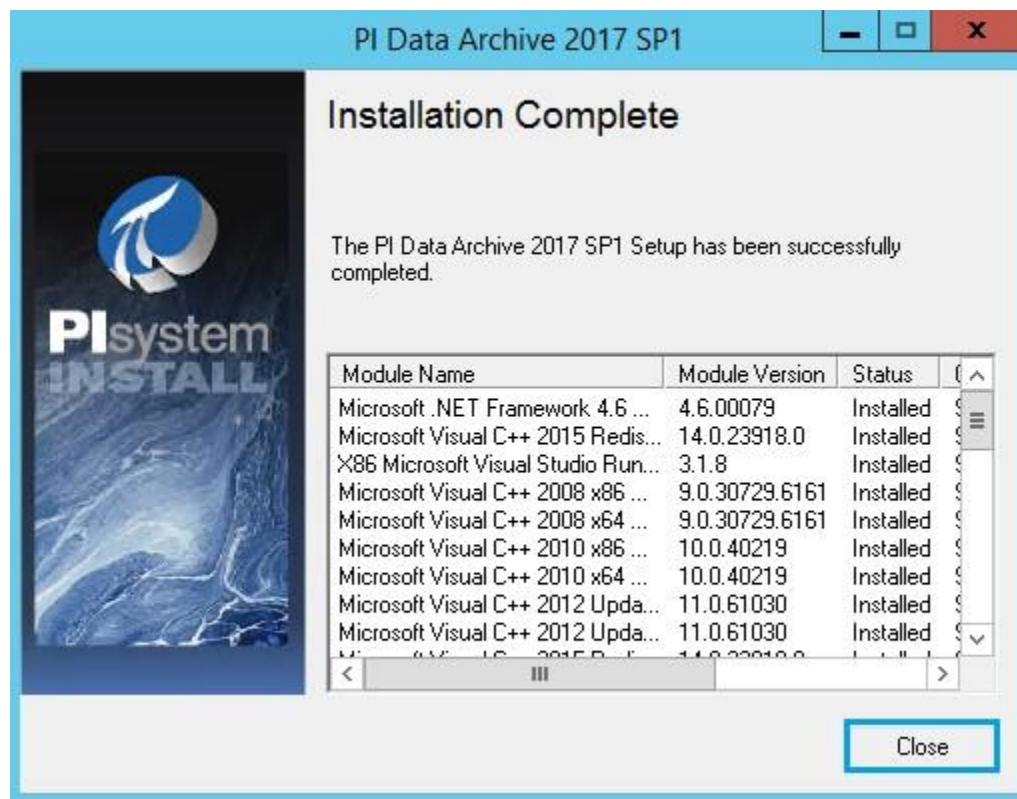
7. Add the domain name to the **Default Asset server** and click on **Next**.



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

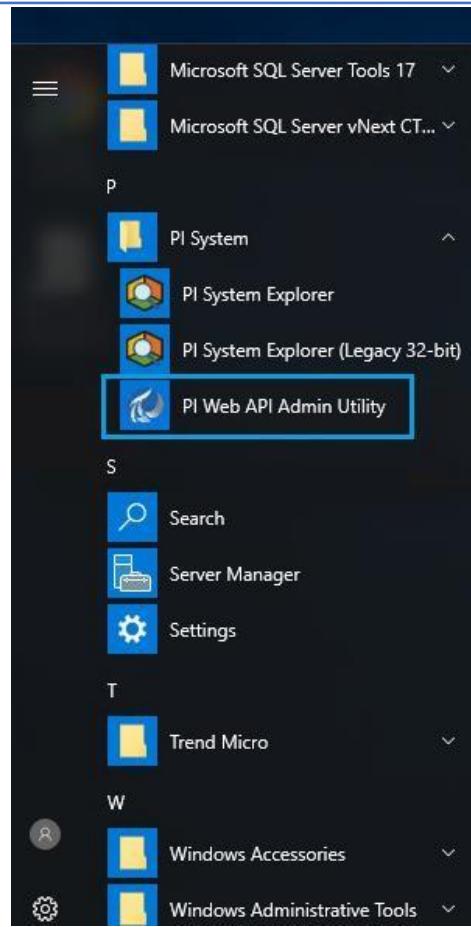


9. Click on **Close** once the installation is completed.

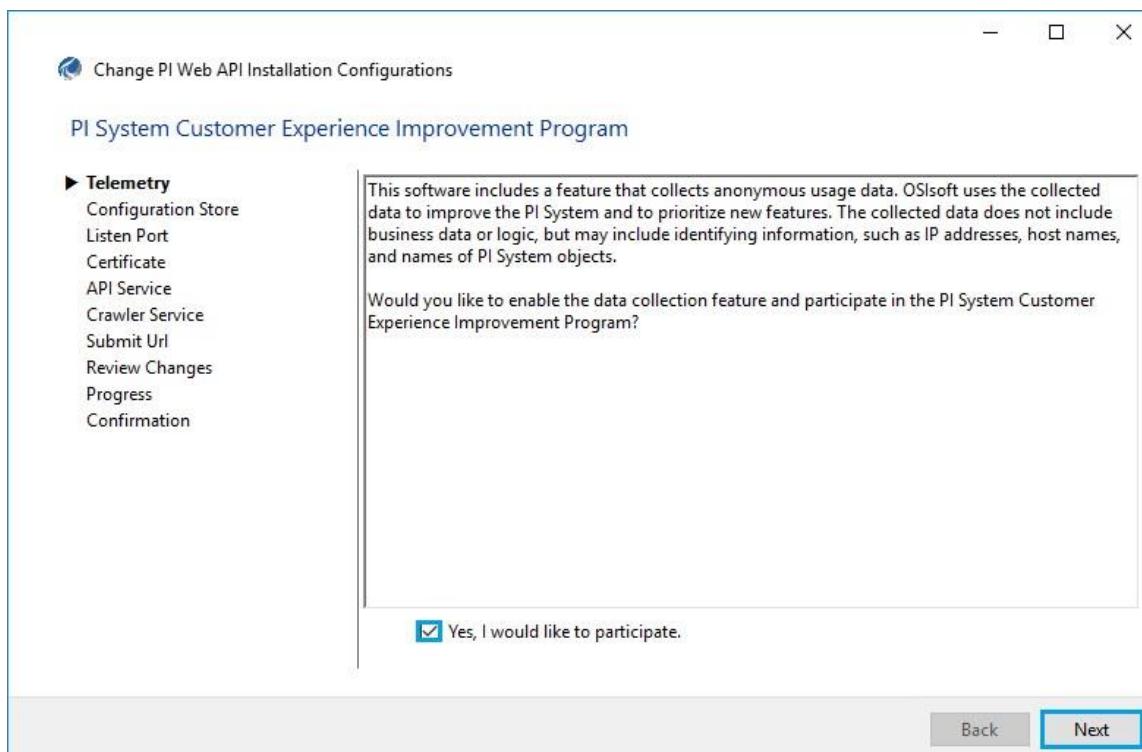


9.3. PI Web API Utility

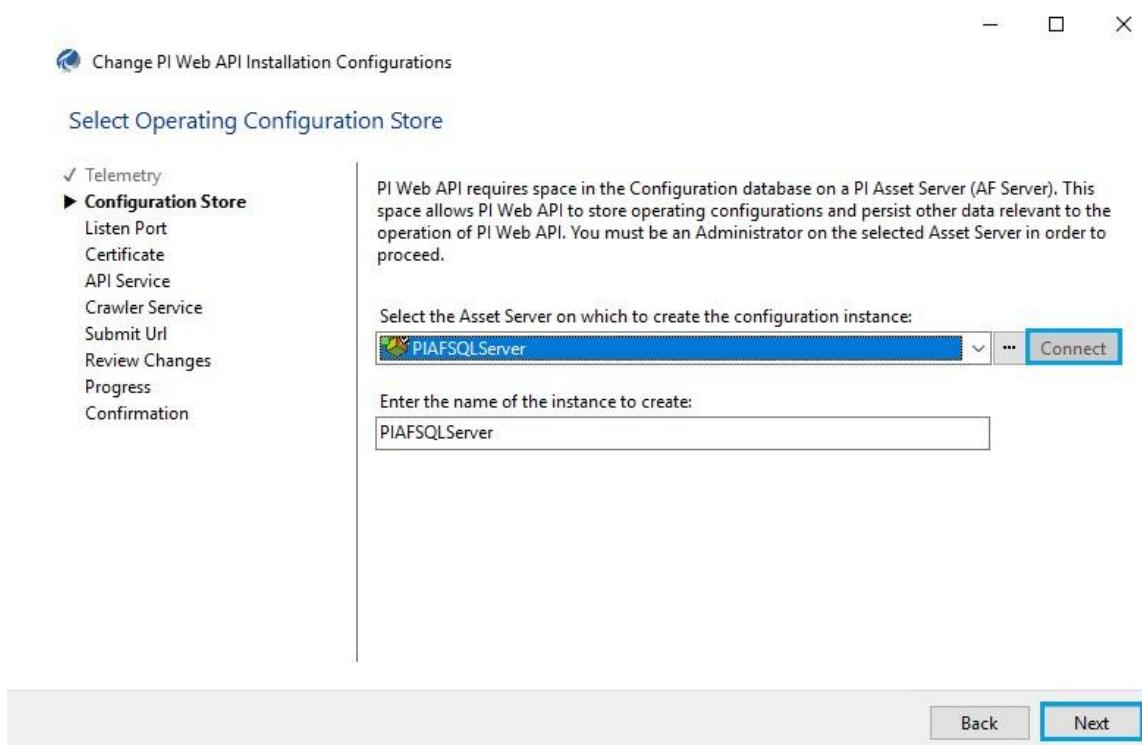
1. Navigate to **PI System > PI Web API Admin Utility** from the Start menu.

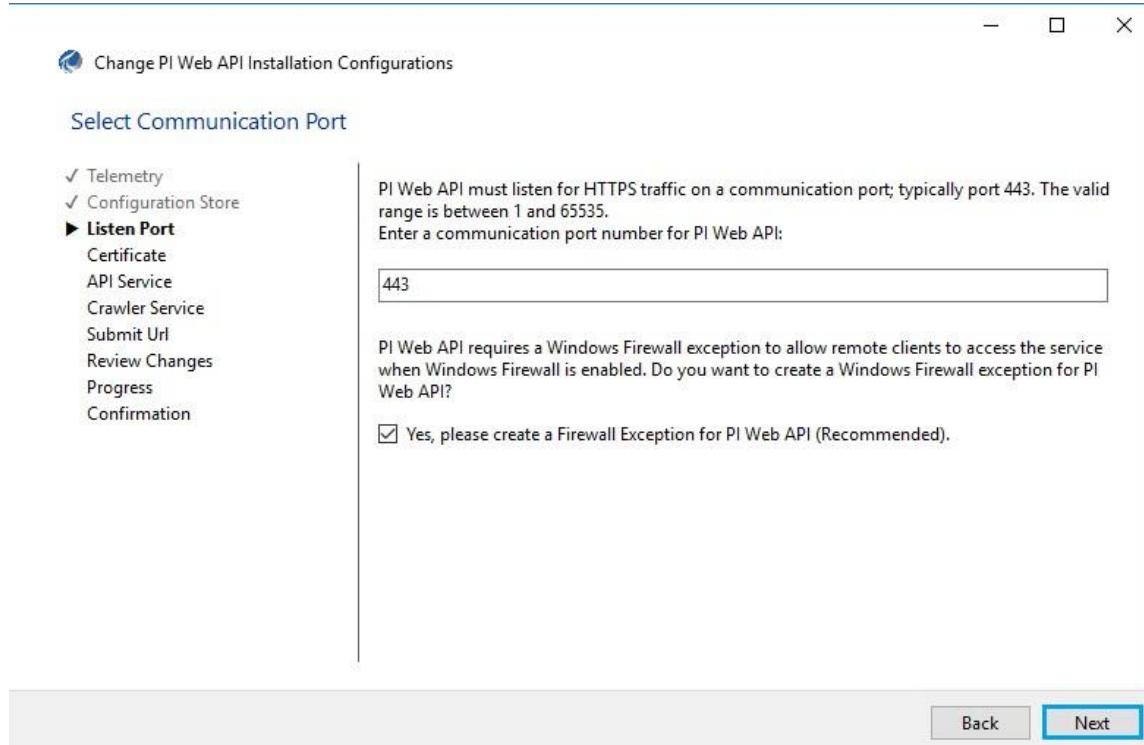


2. Check the **Yes, I would like to participate** dialog box and click on **Next**.



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



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

Change PI Web API Installation Configurations

Select an SSL Certificate for Encrypting Traffic

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

PI Web API requires an SSL certificate to encrypt traffic between the server and clients. If there is no SSL certificate selected or set on the selected listen port, a self-signed certificate will be created and used by PI Web API.

SSL certificate thumbprint:
[4491A55A95344802F0](#)

[Change](#)

PI Web API Admin Utility



A certificate binding is already configured for port 443 on this server. Changing the binding may disrupt existing application running on this computer if they are also using this port. You can keep using the existing certificate for PI Web API.

Do you still want to change the certificate?

[Yes](#)

[No](#)

[Back](#)

[Next](#)

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

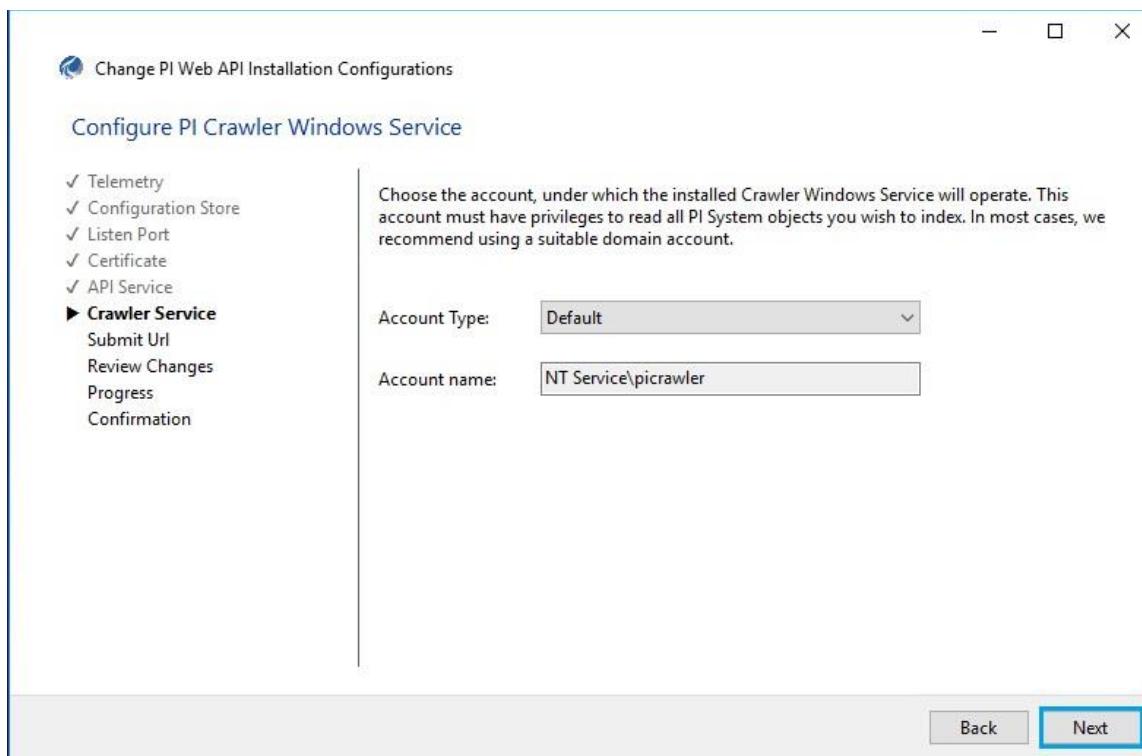
Choose the account, under which the installed API Windows Service will operate. If integrated Windows security (Kerberos) is desired, this account usually must be trusted for delegation in Active Directory. In most cases, we recommend using the default NT Service account.

Account Type:

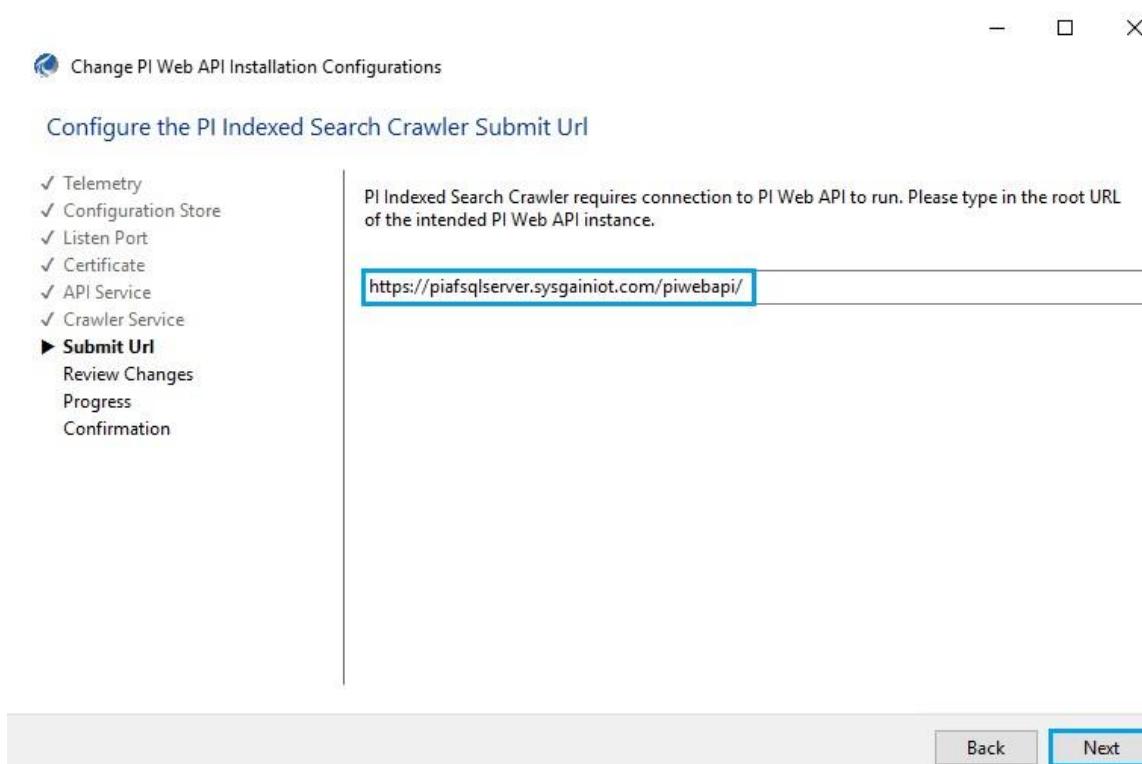
Account name:

[Back](#)

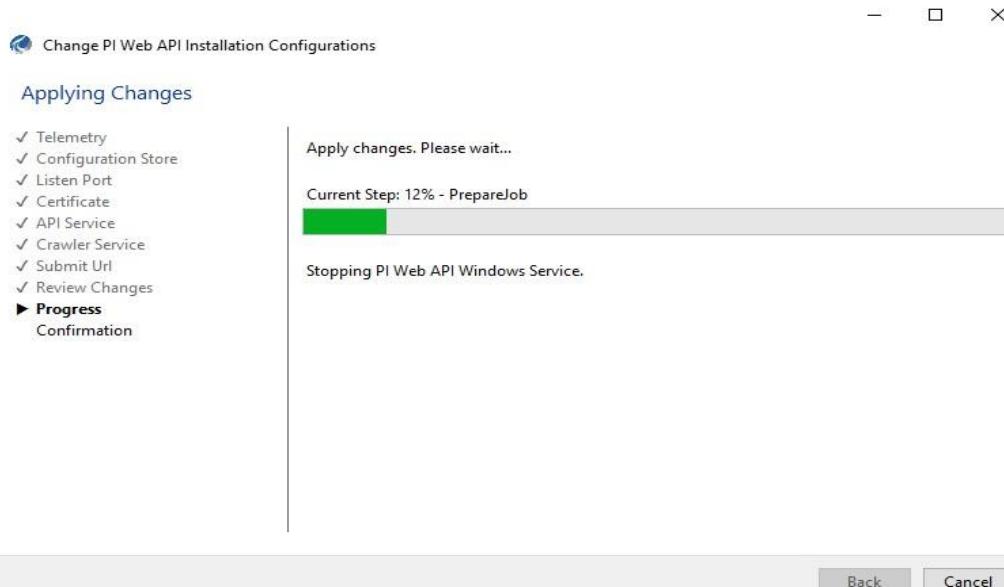
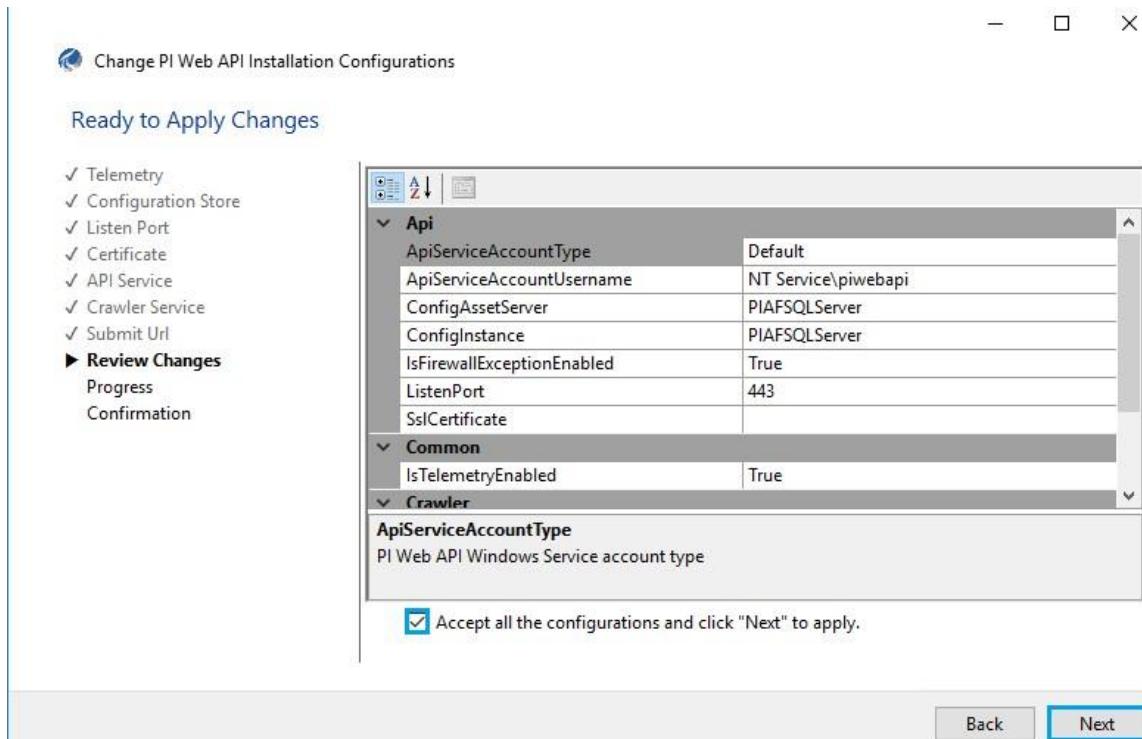
[Next](#)



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**.

Change PI Web API Installation Configurations

Confirmation

✓ Telemetry
✓ Configuration Store
✓ Listen Port
✓ Certificate
✓ API Service
✓ Crawler Service
✓ Submit Url
✓ Review Changes
✓ Progress
► Confirmation

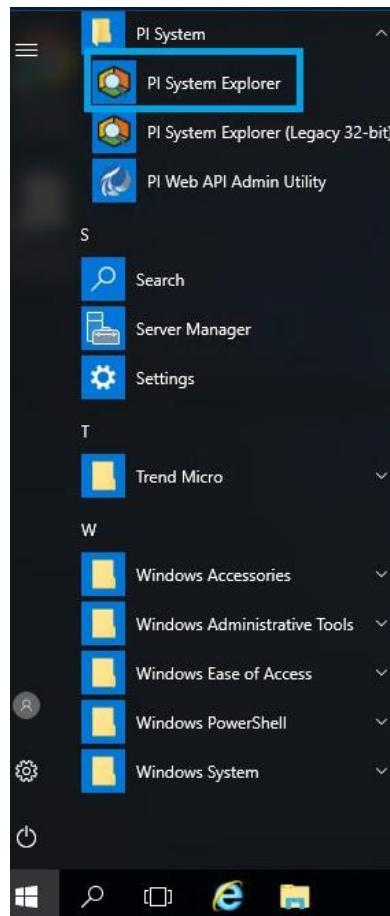
All jobs accomplished successfully.

Job	Result	Note
Prepare Setup Job	Done	
Application Data Folder Setup Job	Done	
Certificate Setup Job	Done	
URL ACL Setup Job	Done	
Listen Port Setup Job	Done	
Firewall Exception Setup Job	Done	
Configuration Store Setup Job	Done	
Complete Setup Job	Done	

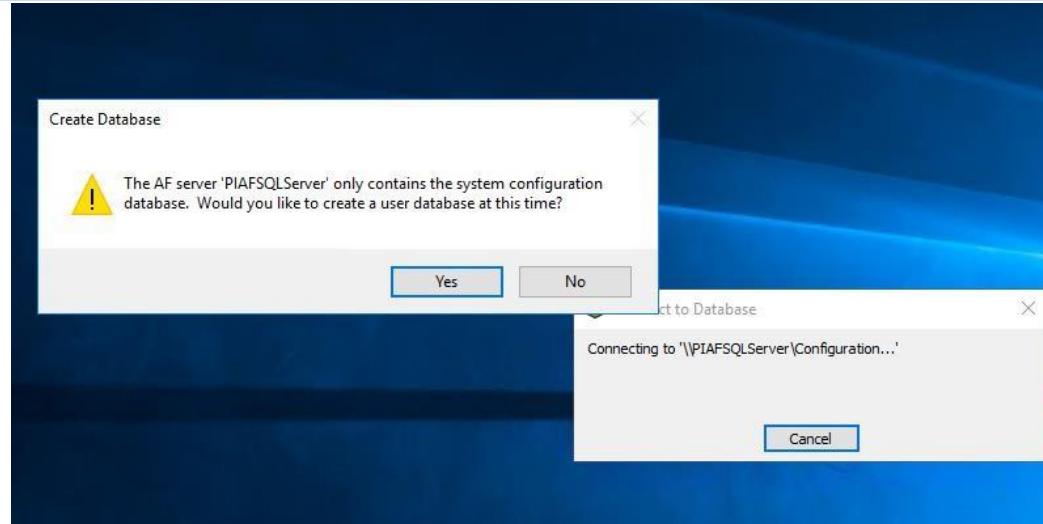
Back Finish

9.4. Creation of Database in PI System Explorer

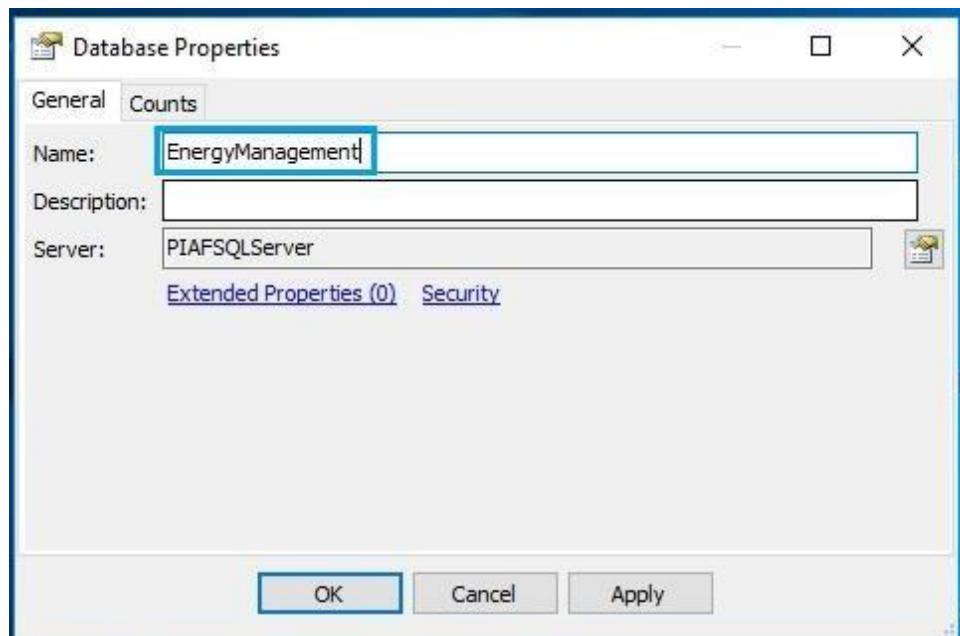
18. On the PIAFSQL machine, Navigate to **PI System Explorer** in PI System folder from the Start menu.



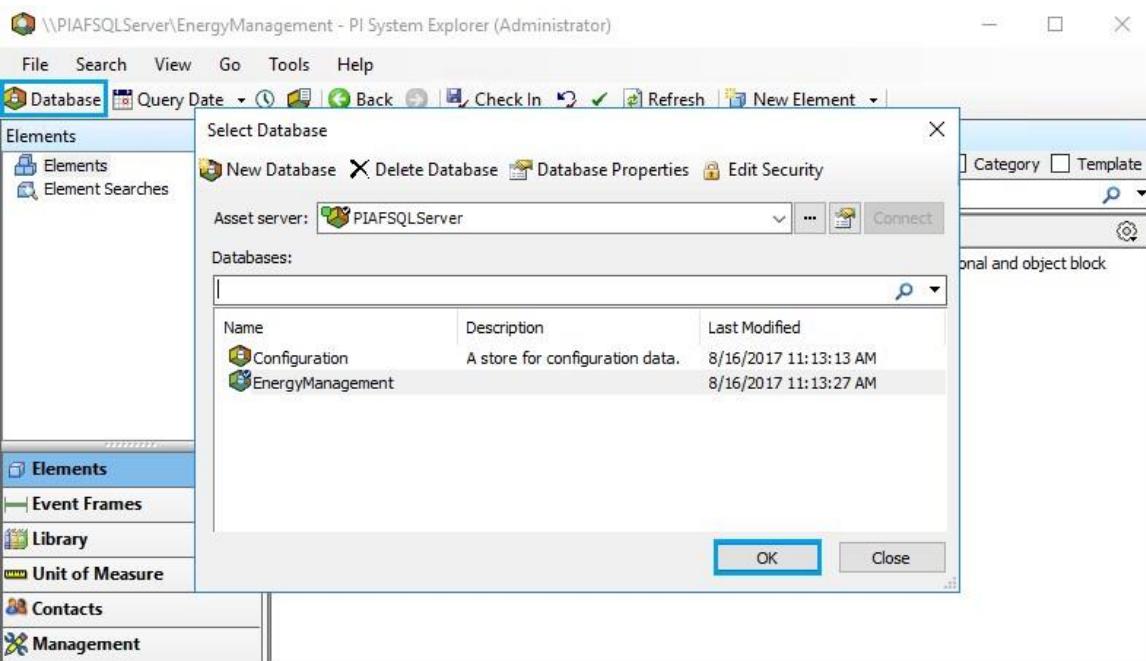
19. Two popups show up, **Connect to Database** and **Create Database**. Click **Yes** on the **Create Database** popup.



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

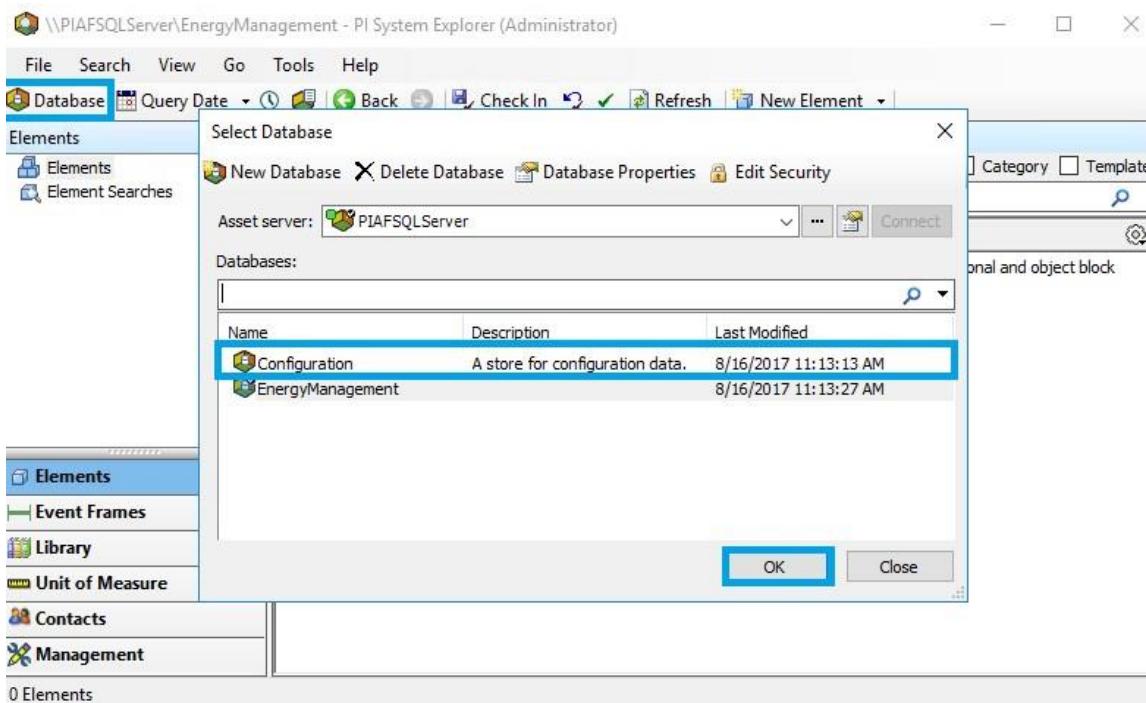


21. Navigate to **PI System Explorer**, click on **Database** to view the created database and click on **OK**.

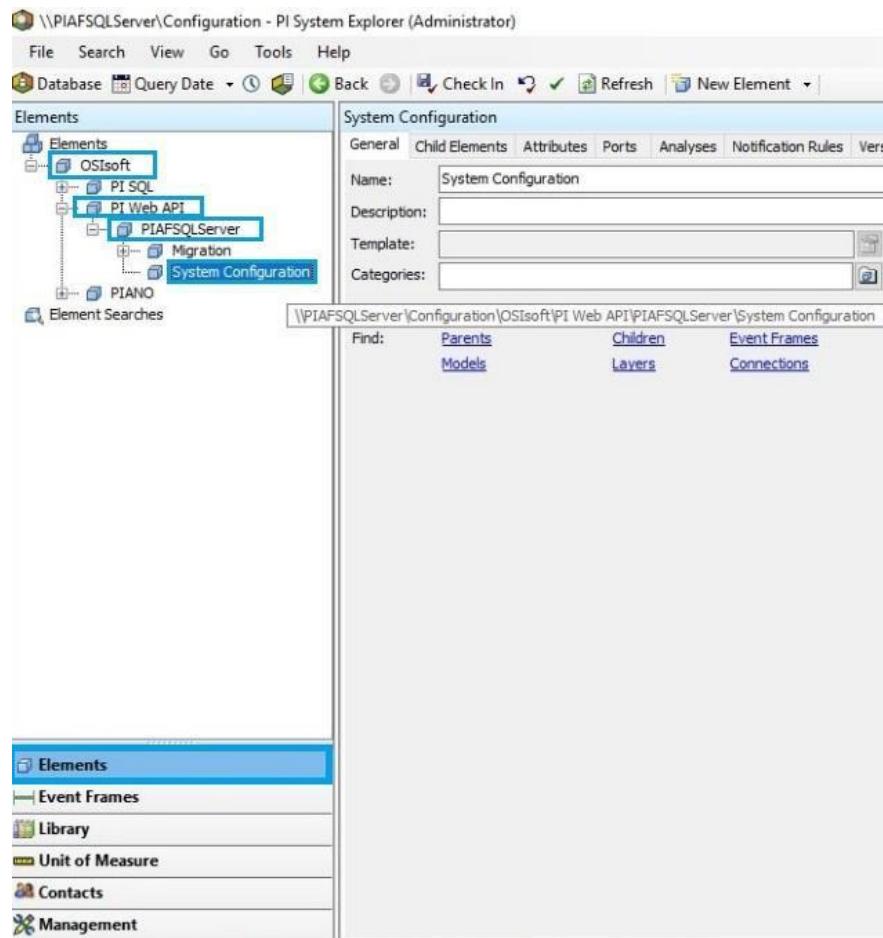


9.5. System Configuration in PI System Explorer

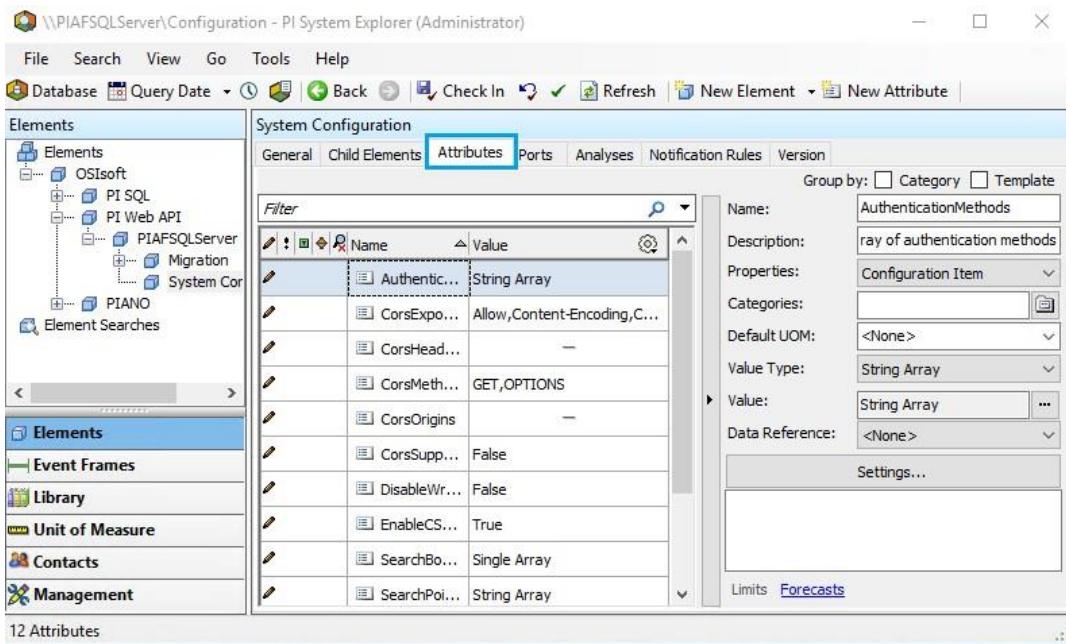
1. Navigate to **PI System Explorer** > Click on **Database** > click **Configuration** under Databases section. Click **OK**.



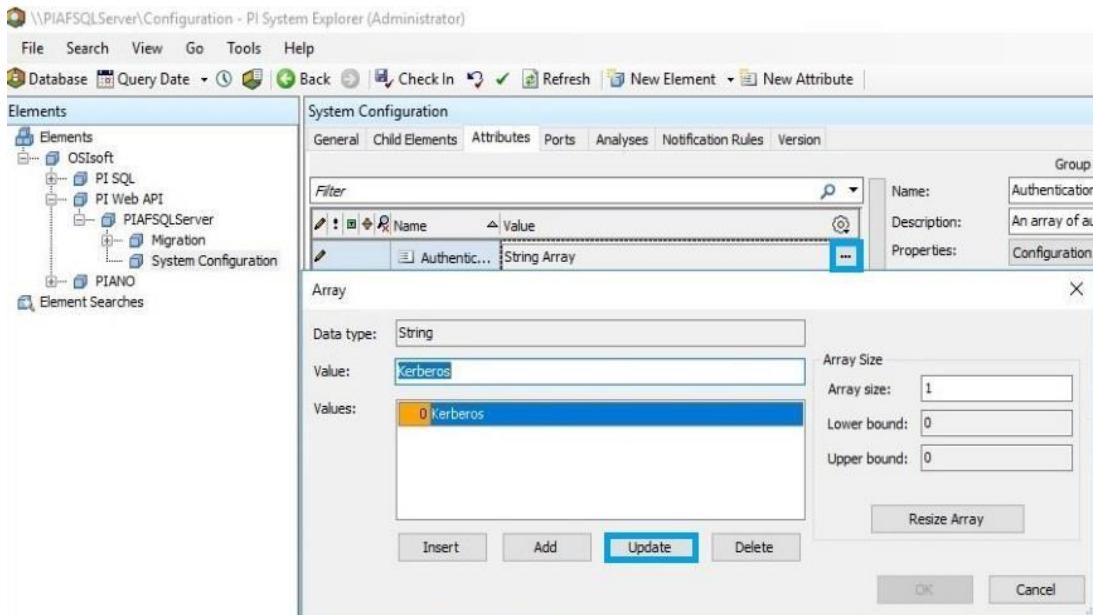
2. Click on **Elements** and navigate to **OSISoft > PI Web API > PIAFSQLServer > System Configuration.**



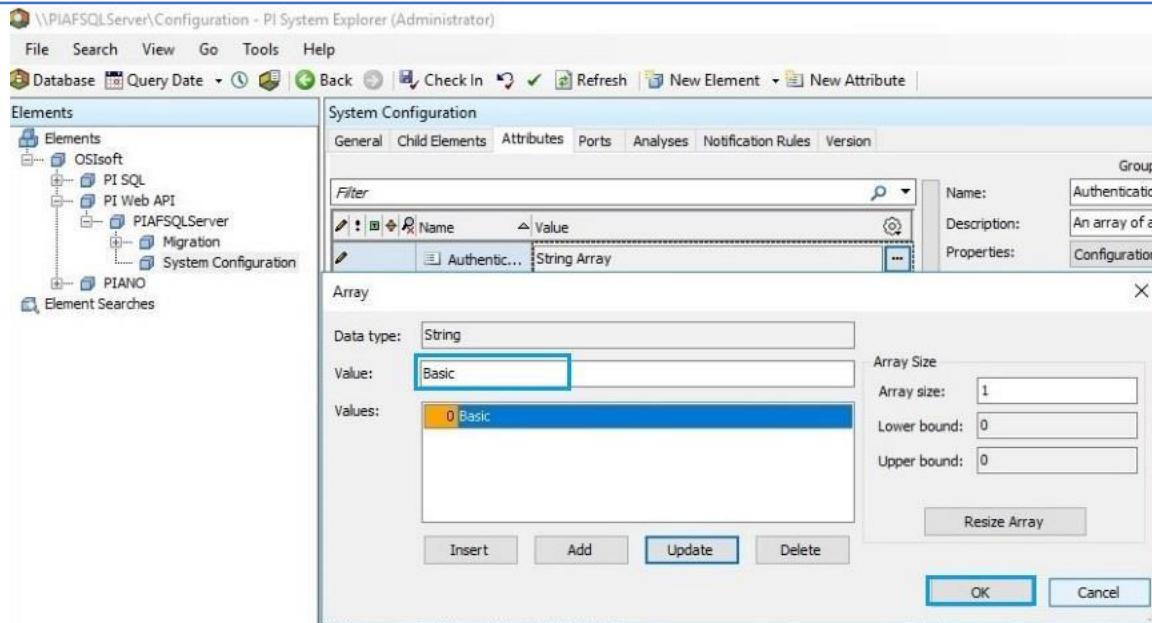
3. Click on **Attributes.**



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

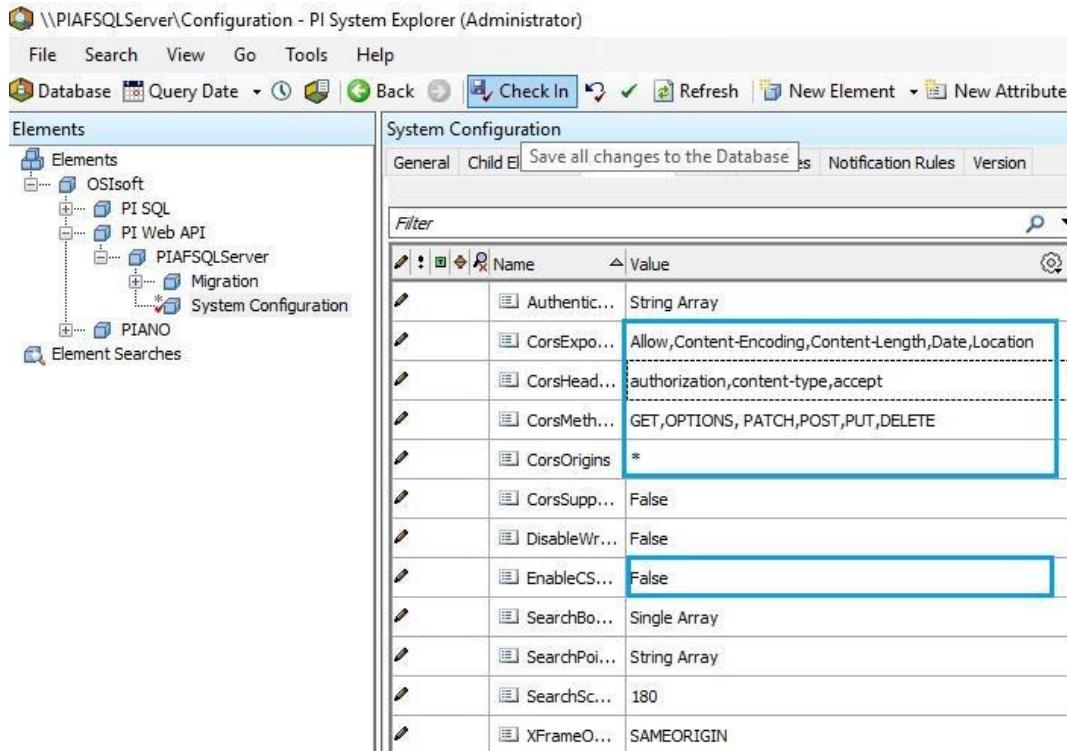


- Click on **Update**, then **OK**.

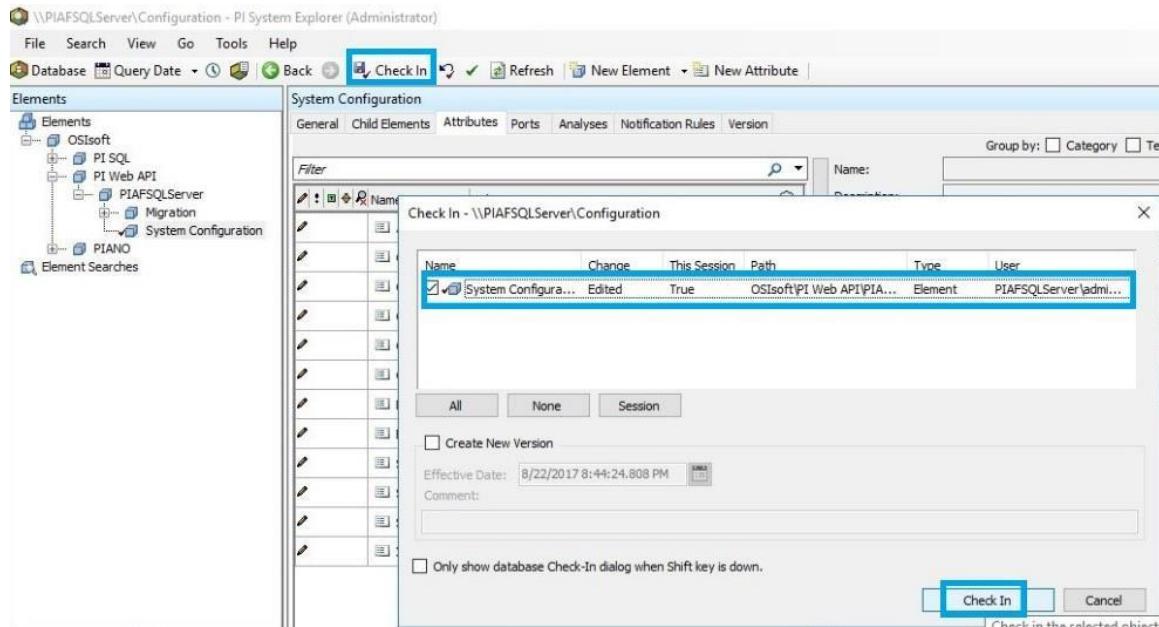


6. Similarly, change the following values:

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

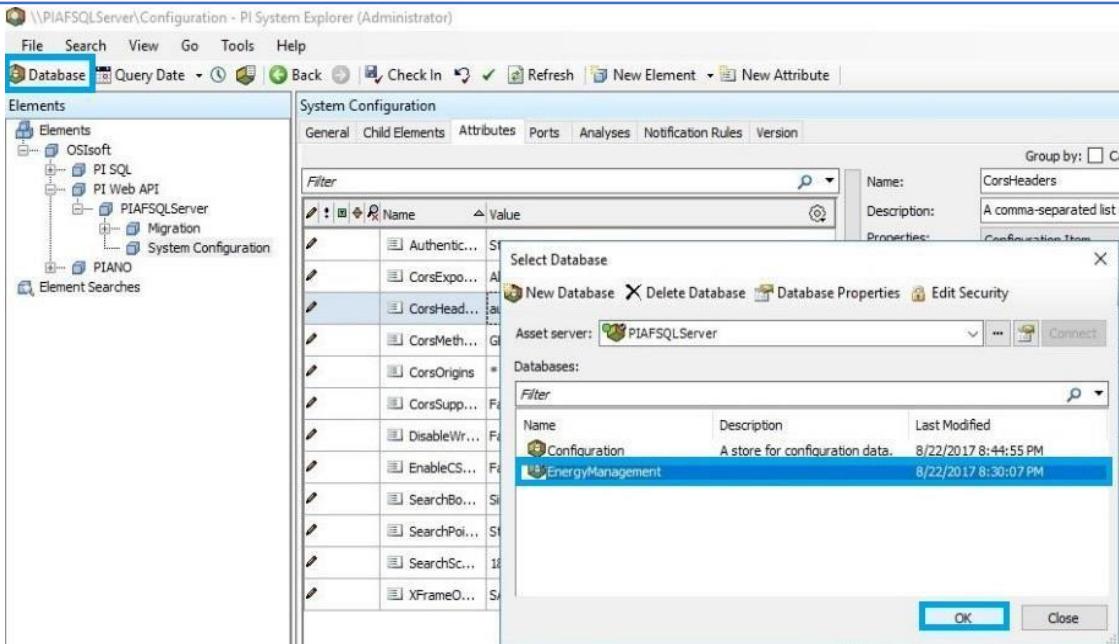


7. Select the **System Configuration** again and click on **Check In**.

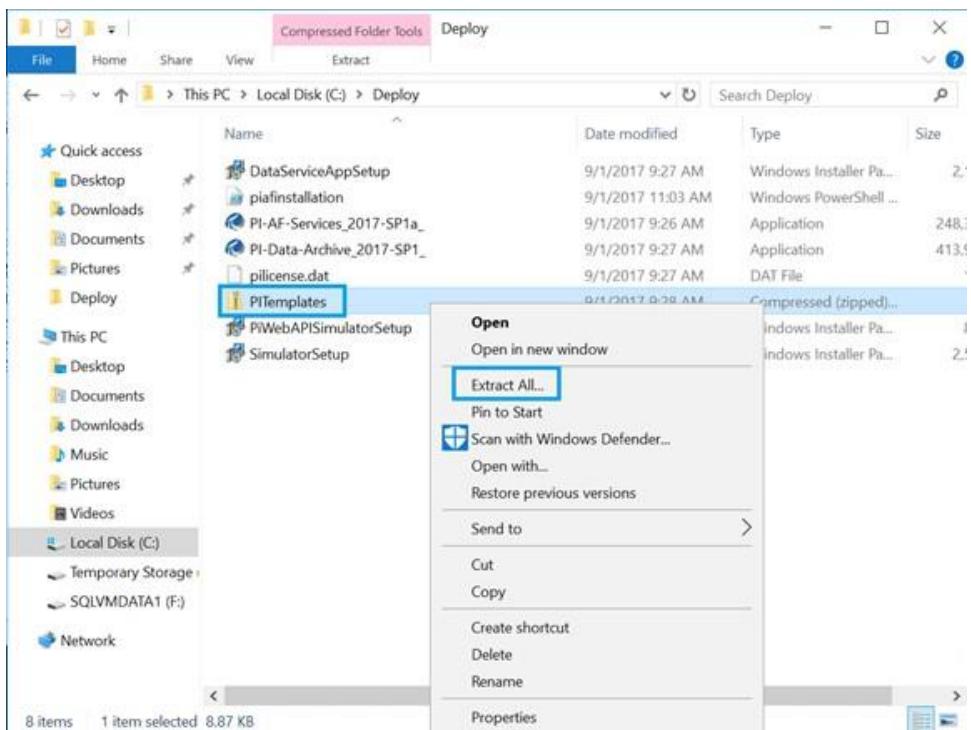


9.6. Import .XML Files into AF Server

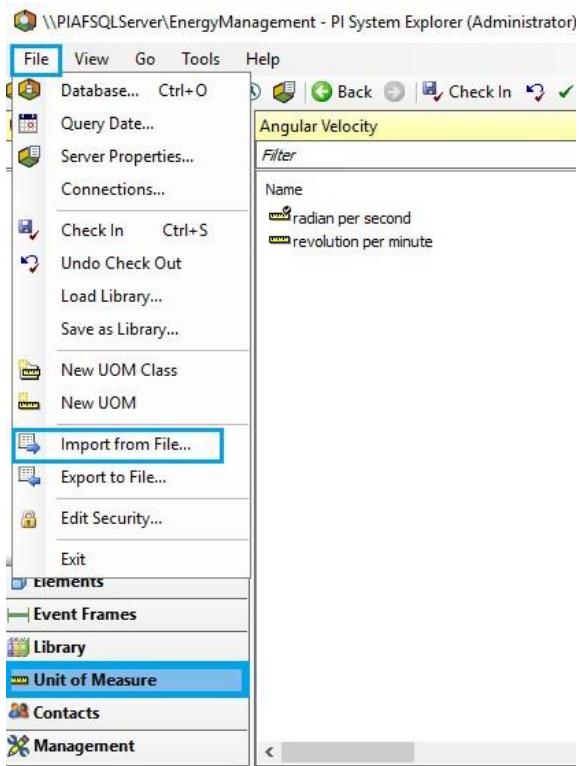
- From the Bastion host connect to the **PIAFSQLServer** virtual machine through the private address with the credentials provided in the output section.
- Navigate to **PI System Explorer > Select Database > Click on Energy Management > Click on OK.**



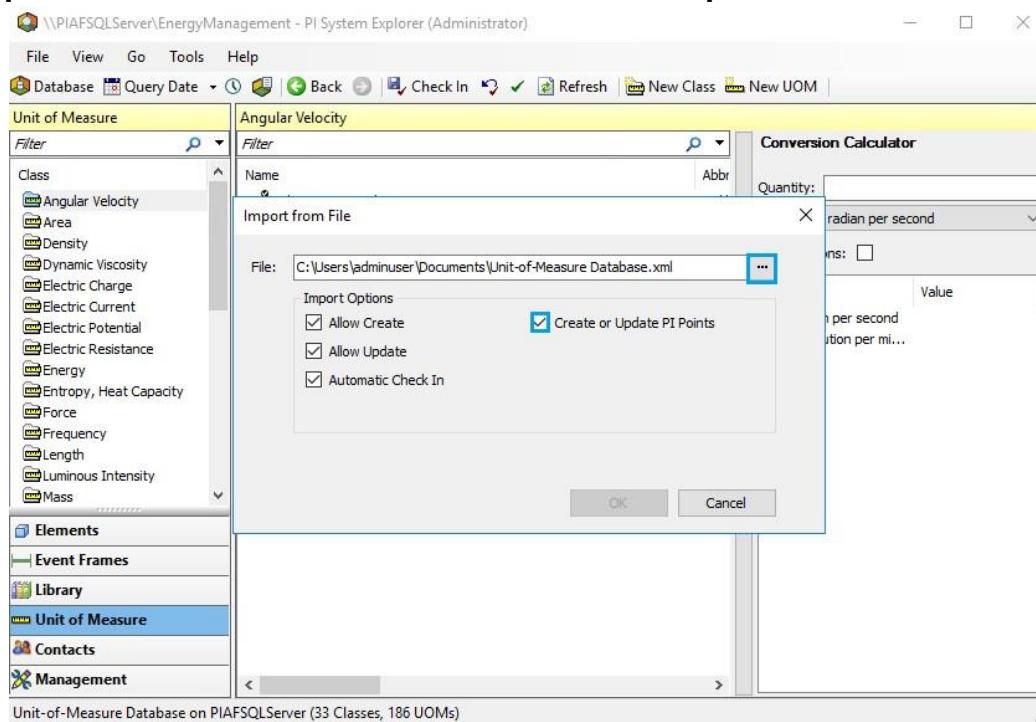
3. Navigate to Local disk (C:) > Deploy > unzip PI templates.



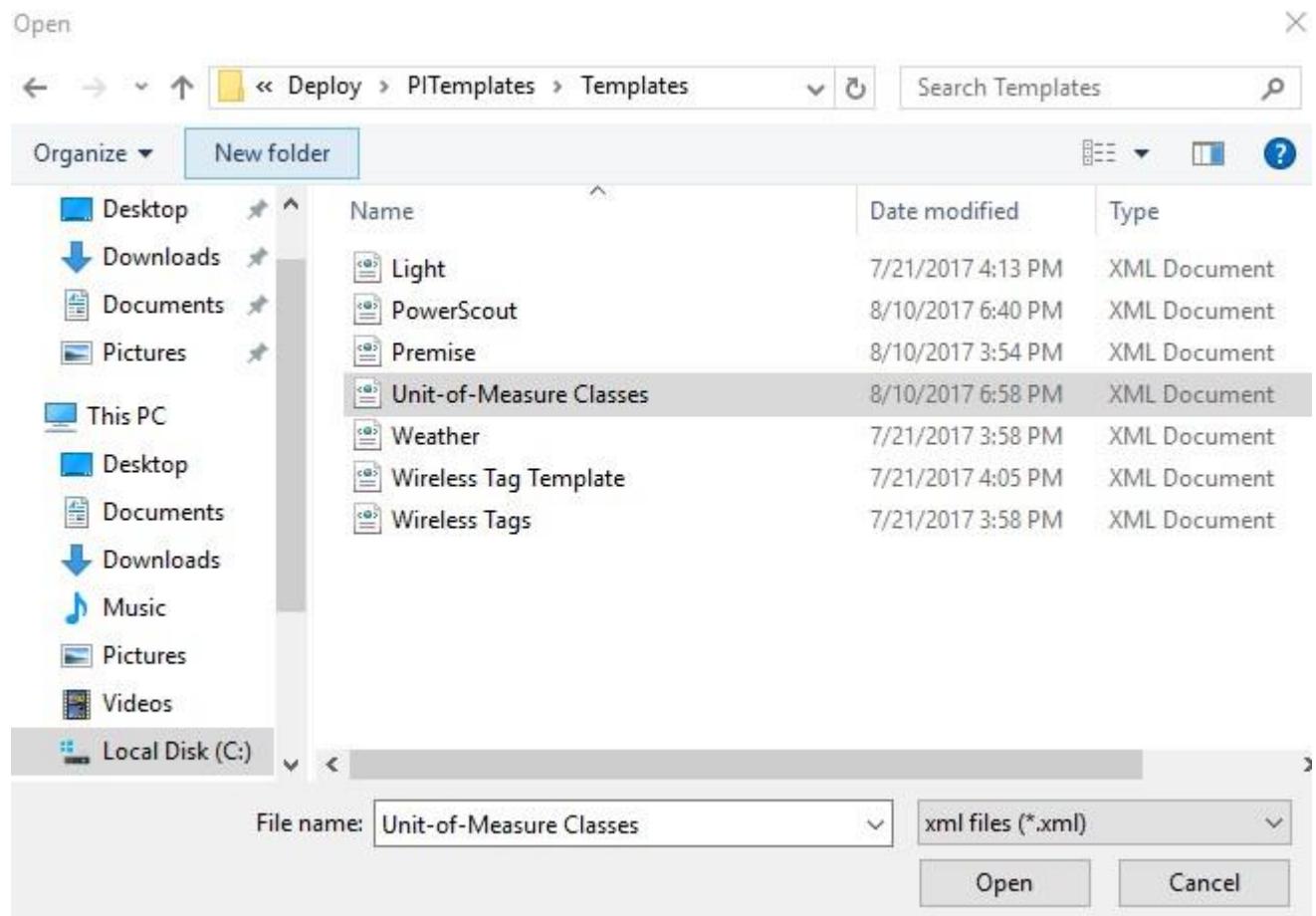
4. Select Unit of Measure > File > Import from file



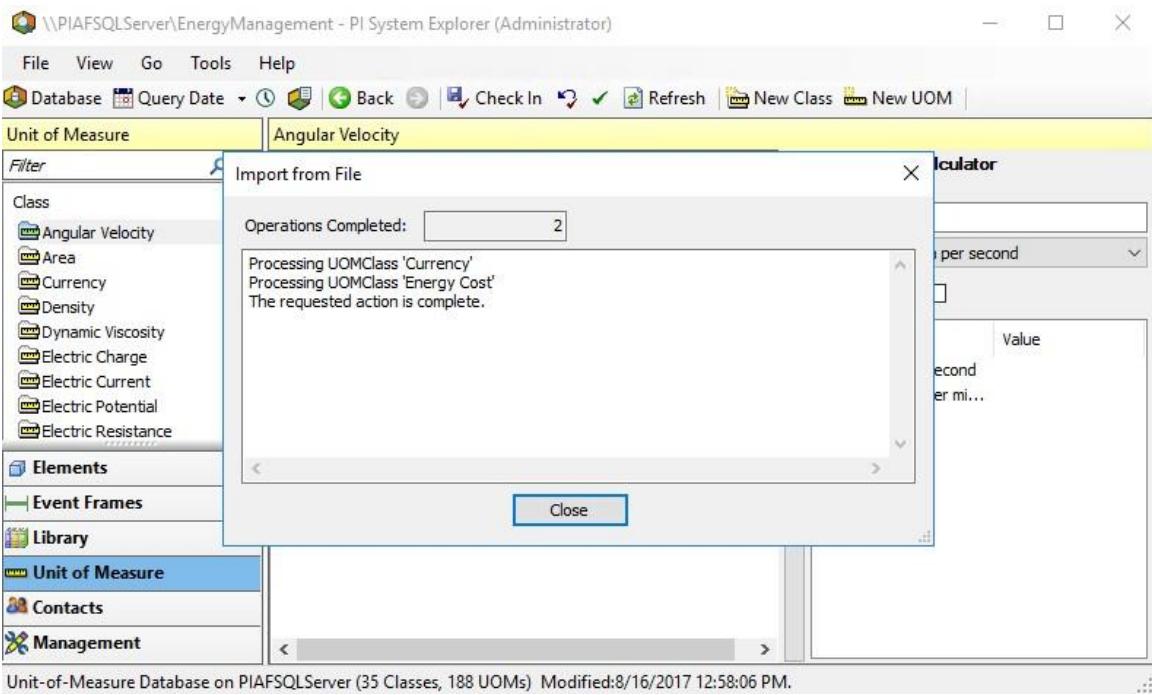
- Check the box for **Create or Update the PI Points** > browse to **local disk (C:)** > **Deploy** > **PITemplates** > Select **Unit of Measure Classes** > Click on **Open**.



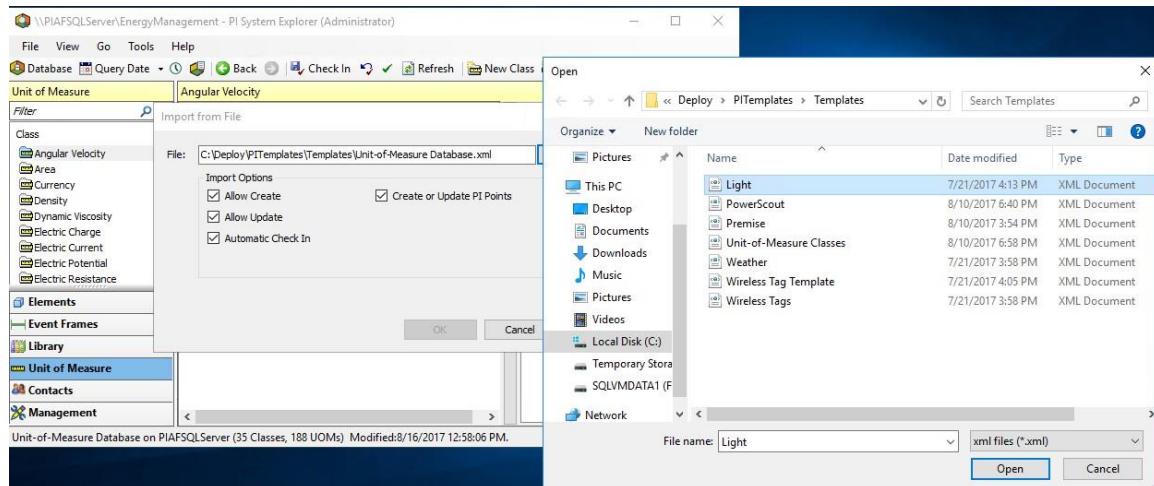
After Open click on ok.



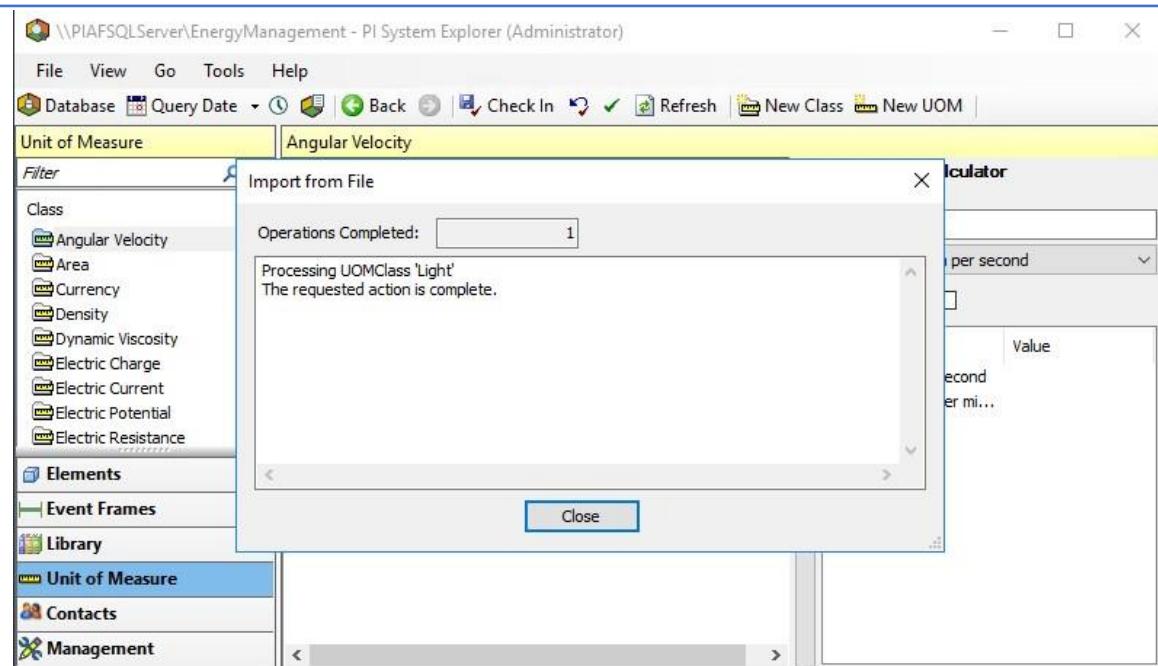
6. You can find the status of the completed operation. Click on **Close**.



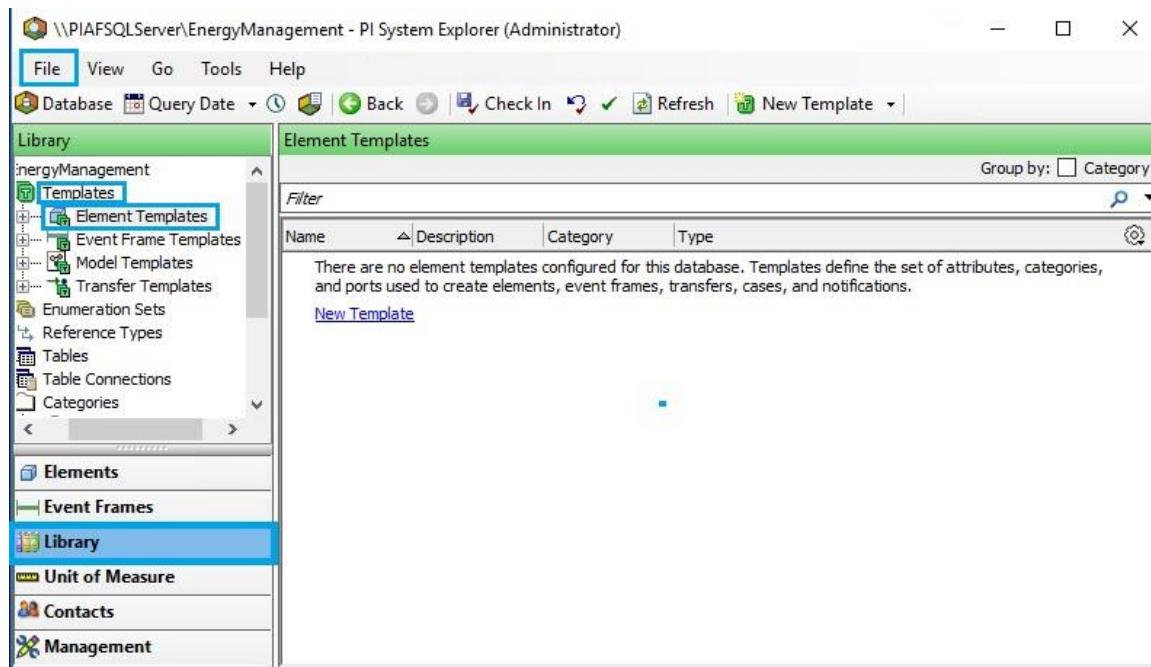
- Again click on the import from file from file menu Check the box **Create or Update the PI Points** > browse to **C:\Deploy\PITemplates** > Select **Light** and click on **Open**.



- 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

Search

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

Group by: Category Template

Elements

Event Frames

Library

Unit of Measure

Contacts

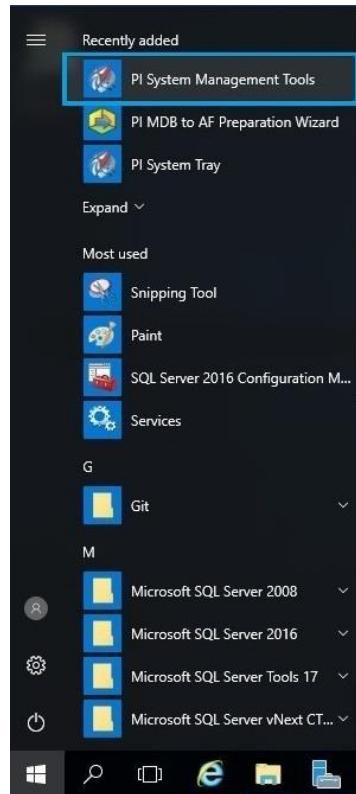
Management

3 Elements

A screenshot of the PI System Explorer application window. The title bar shows the path '\PIAFSQLServer\EnergyManagement'. The menu bar includes File, Search, View, Go, Tools, and Help. The toolbar has Database, Query Date, Back, Check In, Refresh, and New Element buttons. A search bar at the top right says 'Search Elements' with a magnifying glass icon. On the left, a tree view under 'Elements' shows 'Premise', 'Weather', 'Wireless Tags', and 'Element Searches'. Below this is a 'Search' section with a table displaying three rows: 'Premise', 'Weather', and 'Wireless T...'. The table has columns for Name, Description, Category, Type, and Template. At the bottom left is a sidebar with links for Elements, Event Frames, Library, Unit of Measure, Contacts, and Management, with 'Elements' being the active tab. A status bar at the bottom left says '3 Elements'.

9.7. Update Security in PI System Management Tools

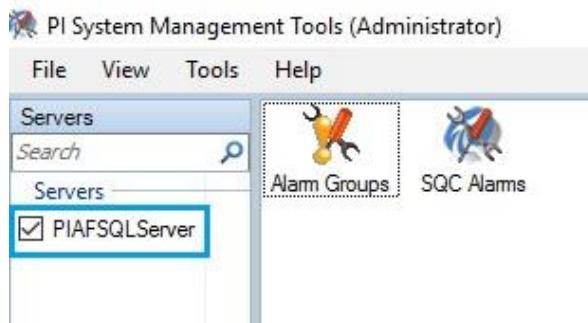
1. From the Start menu, open the **PI System Management Tools**.



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



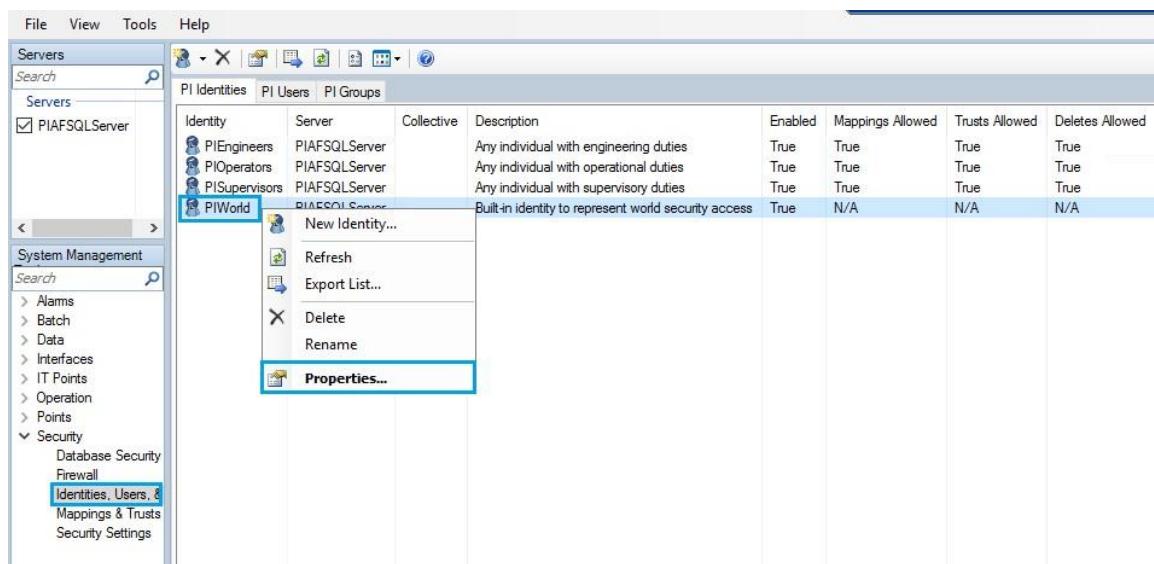
- Under Servers, check the **PIAFSQLServer** box.



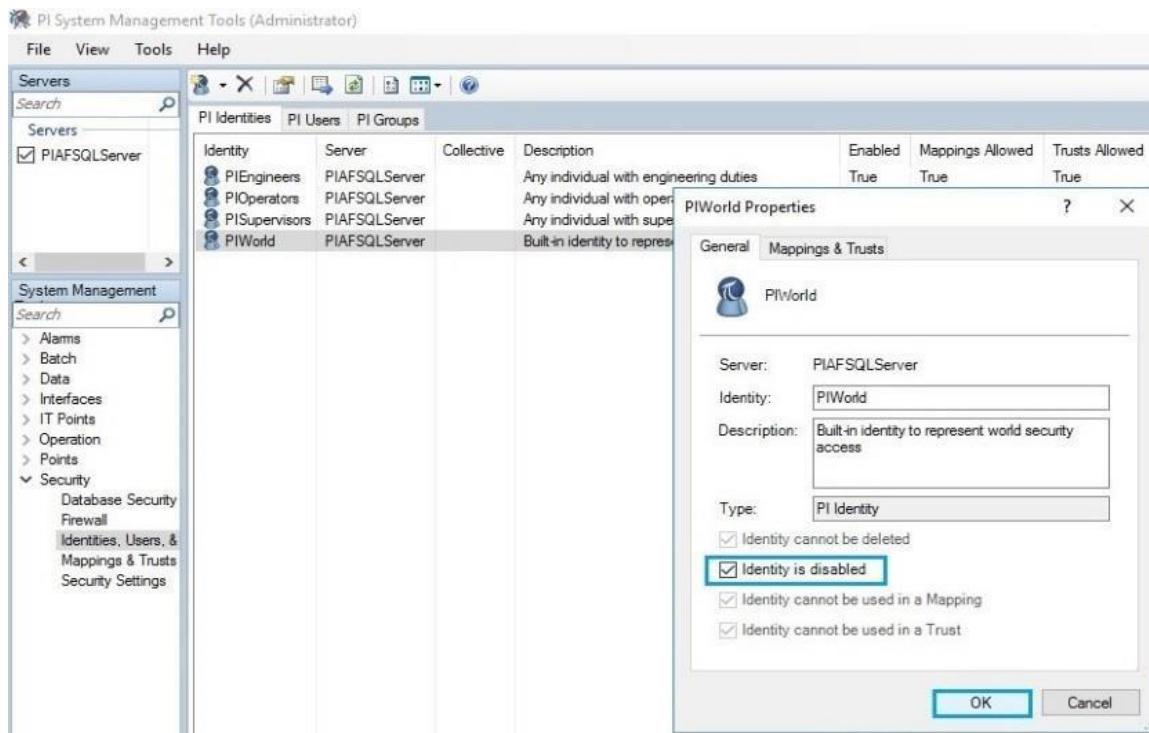
- Click on **Security** under **System Management**, then click on **Security Settings**.



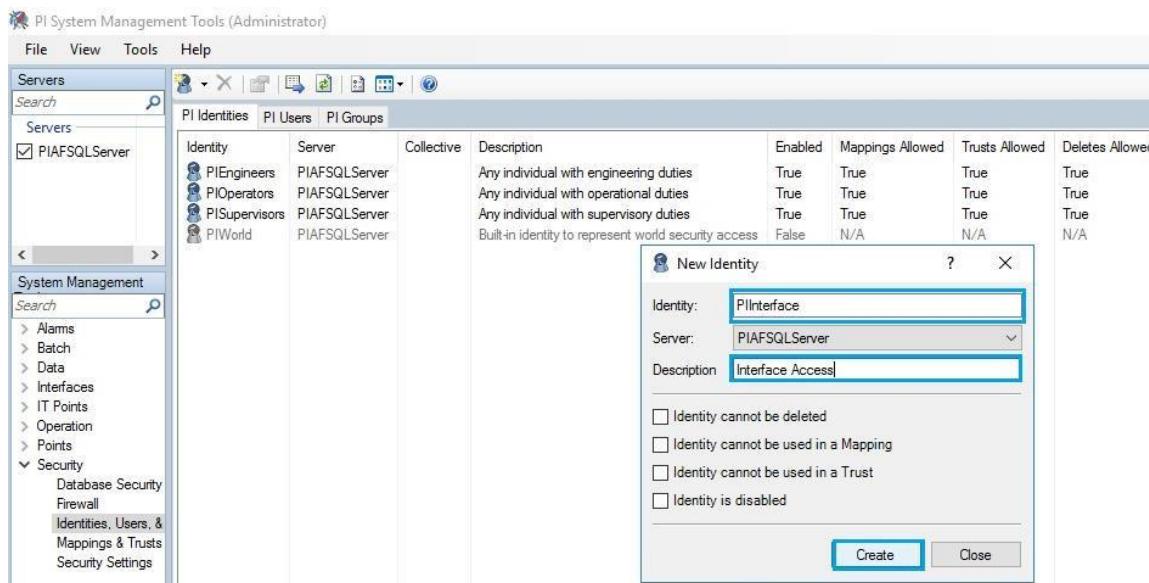
- Click on **Identities, Users and Groups**, then right-click on **PIWorld** under PI identities and select **Properties**.



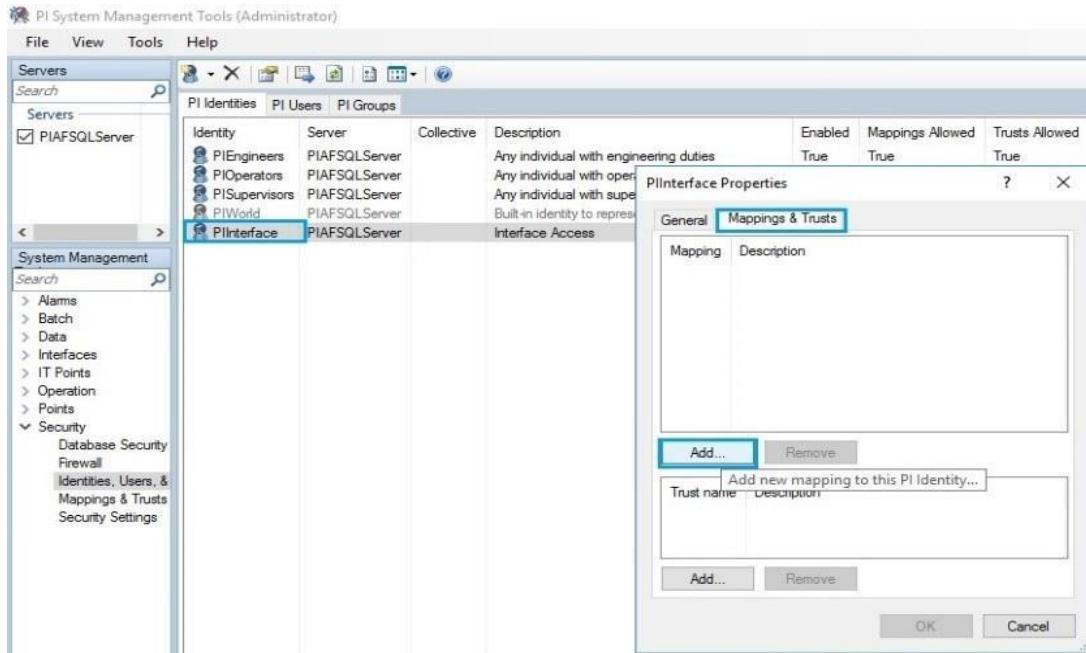
6. Select the **Identity is disabled** checkbox and click on **OK**.



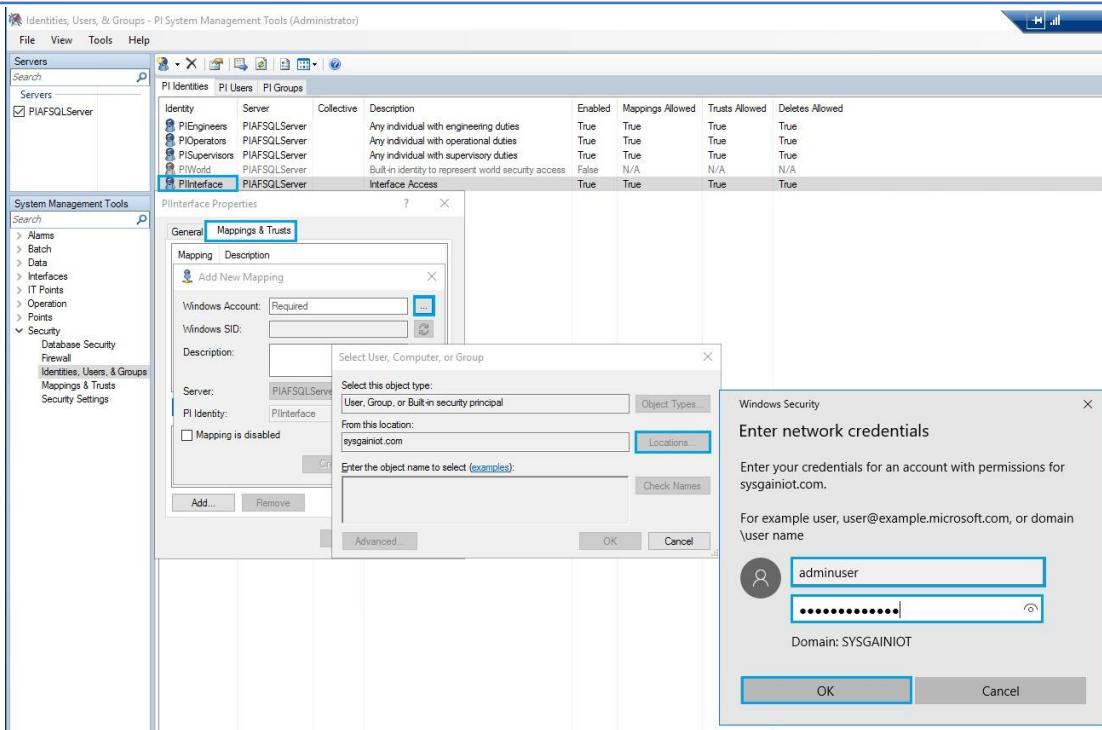
7. The **Enabled** column under **PIWorld** will appear as **False**.
 8. Right-click **PI Identities** to create a new identity. Give the identity the name **PIInterface** and the description **Interface Access**, then click on **Create**.



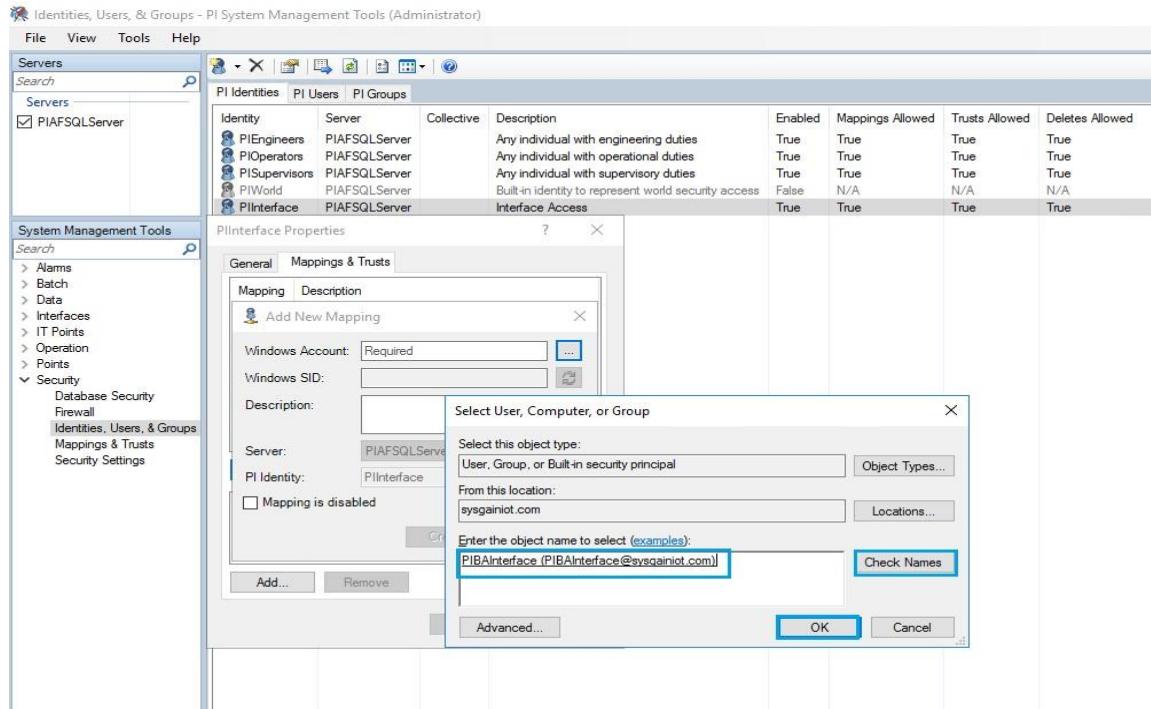
9. Right-click on the newly created **PIInterface** identity, then go to **Properties > Mappings & Trusts**, then click on **Add**.



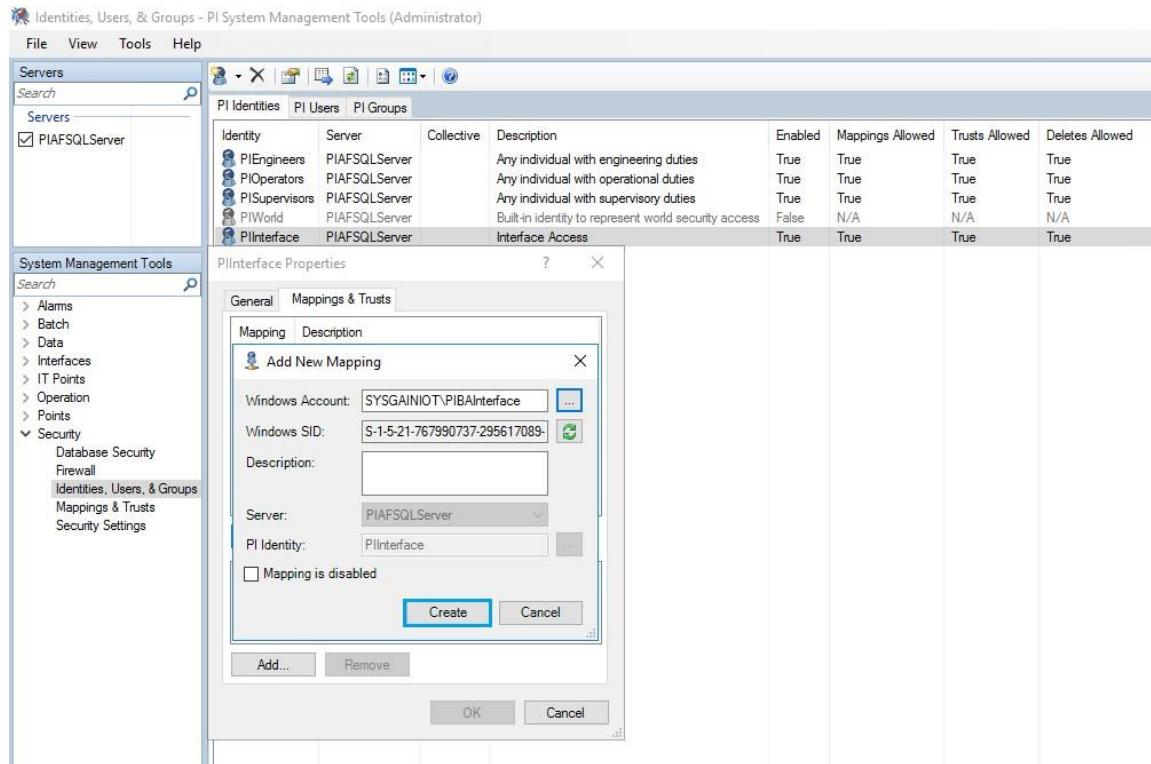
10. After click on **Add** it will show the popup box Add new mapping in that **Browse** at end of **Windows Account** again it will show the popup box as select user,computer,or group in that click on **Locations**. select the domainname Enter the credentials and click on **OK**



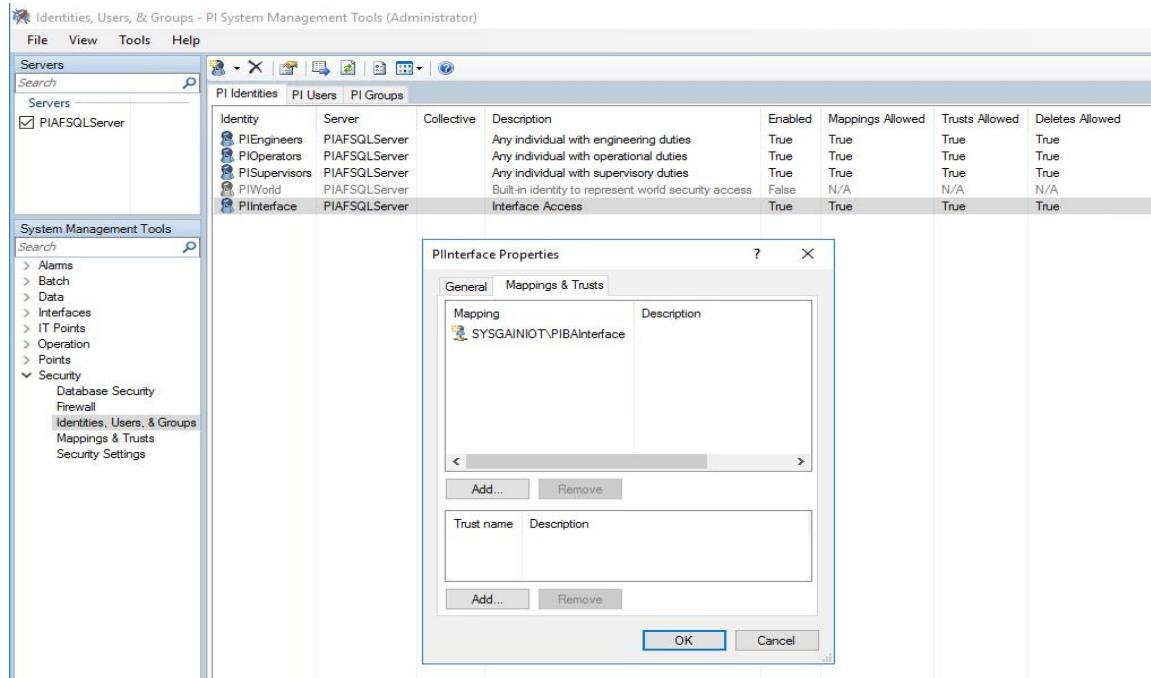
11. Give object name as **PIBAInterface** > **Click on Check Names** > **OK**



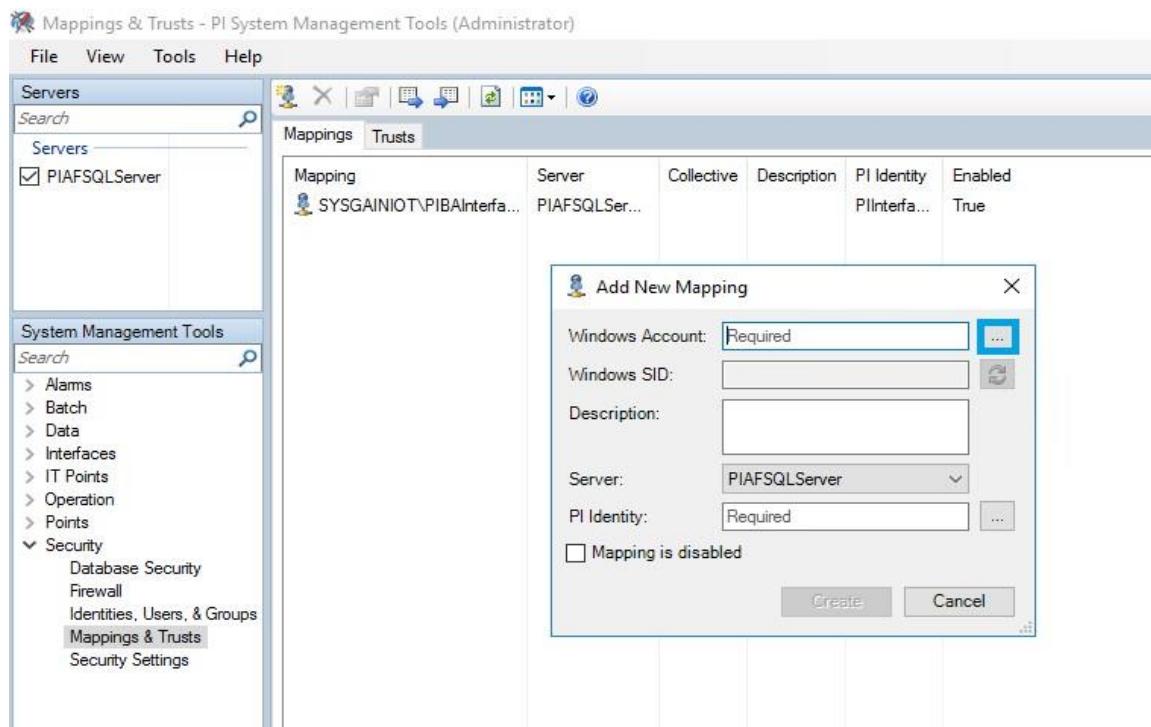
12. Click on **Create** to create a New Mapping for PIBAInterface.



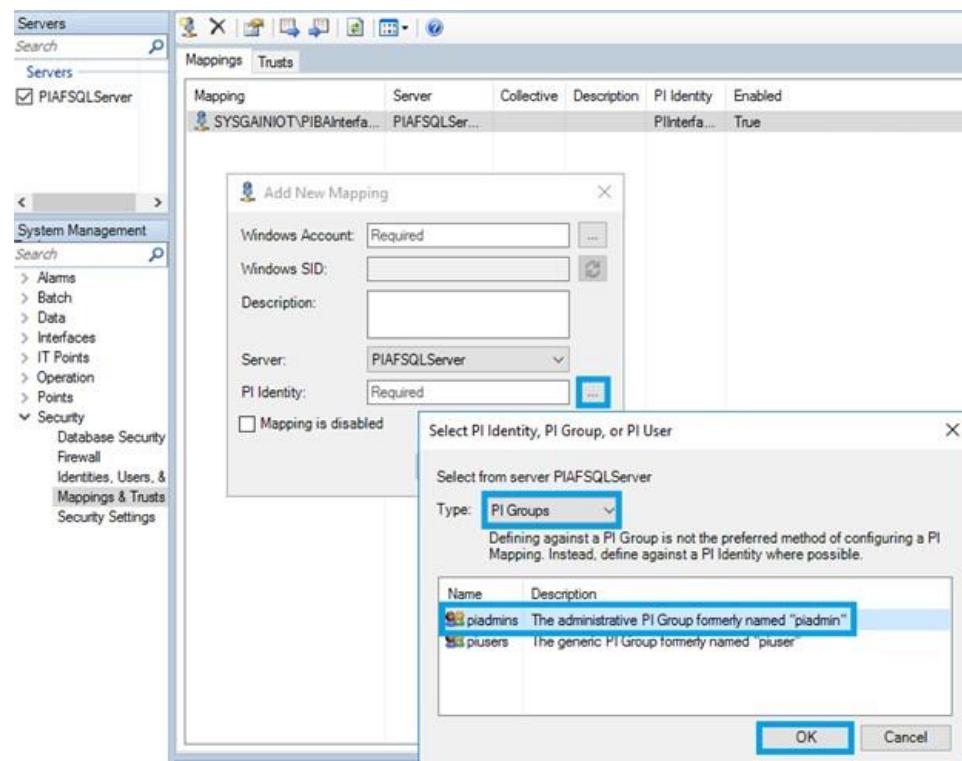
13. Click **OK** once the PIBAInterface mapping is created.



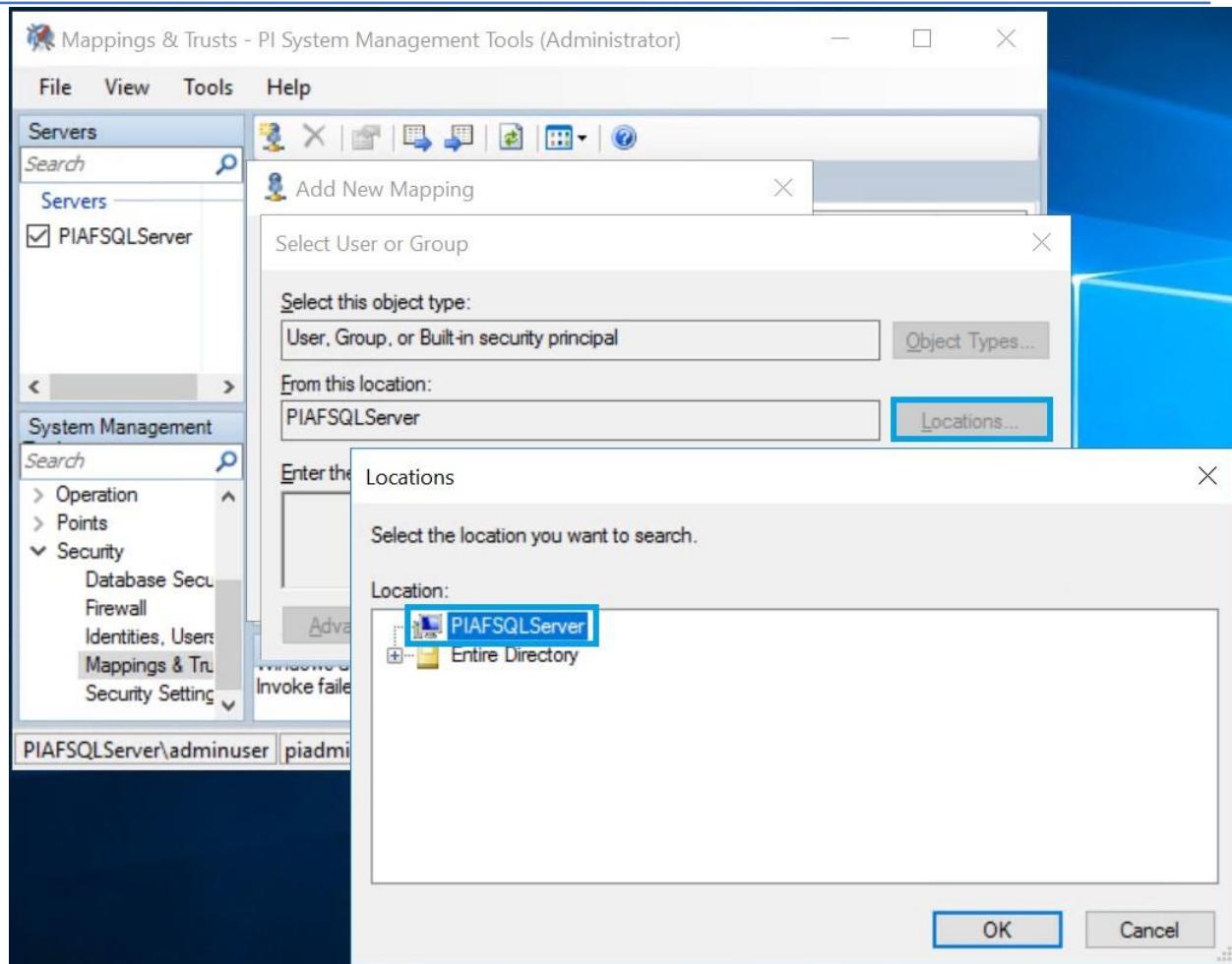
14. Navigate to **Security > Mapping & Trusts** to create a New Mapping. Click on the mappings above symbol to add new mapping.



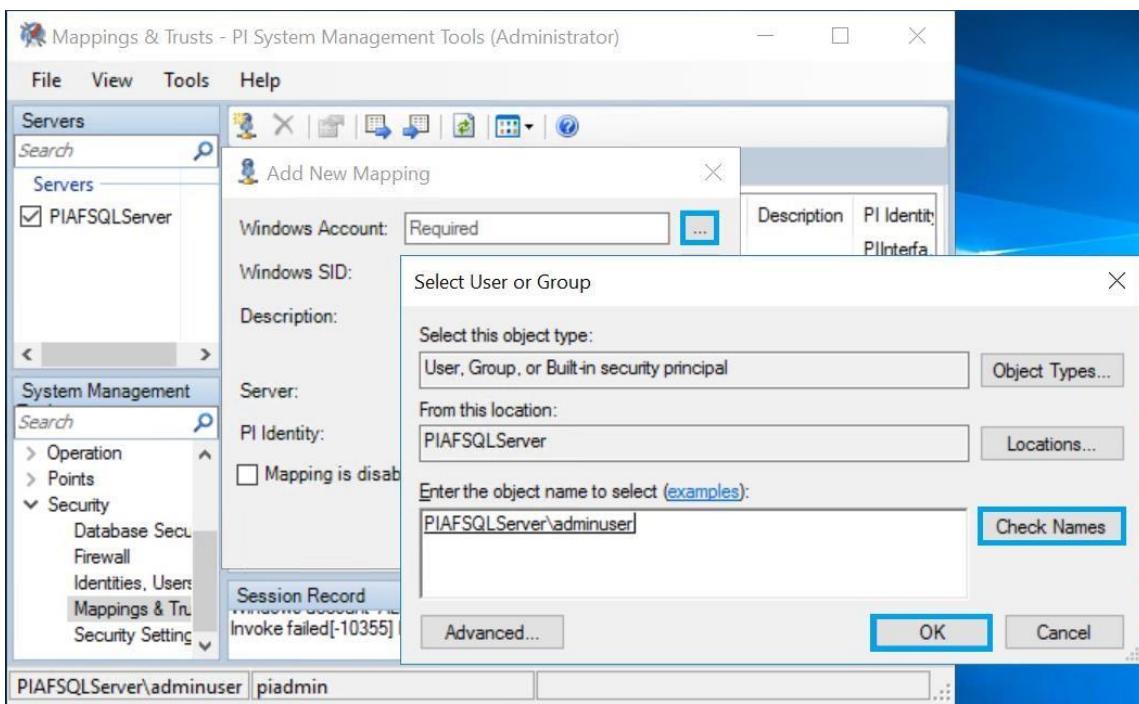
15. Browse the directory in **PI Identity** section, then select **PI groups** under the **Type** dropdown and Select **piadmins** to create PI Identity as **piadmins** click on **OK**.



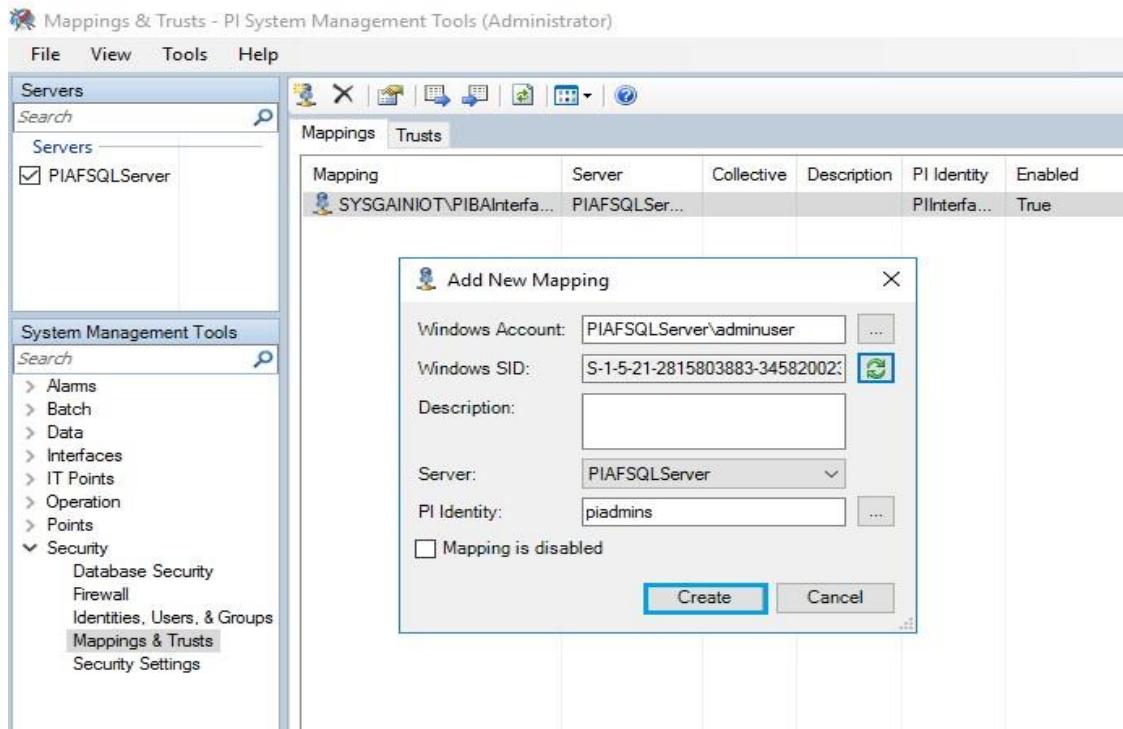
16. Click the dots next to **Windows Account**, then **Locations**, and select the **PIAFSQLServer**.
 Click on **OK**.



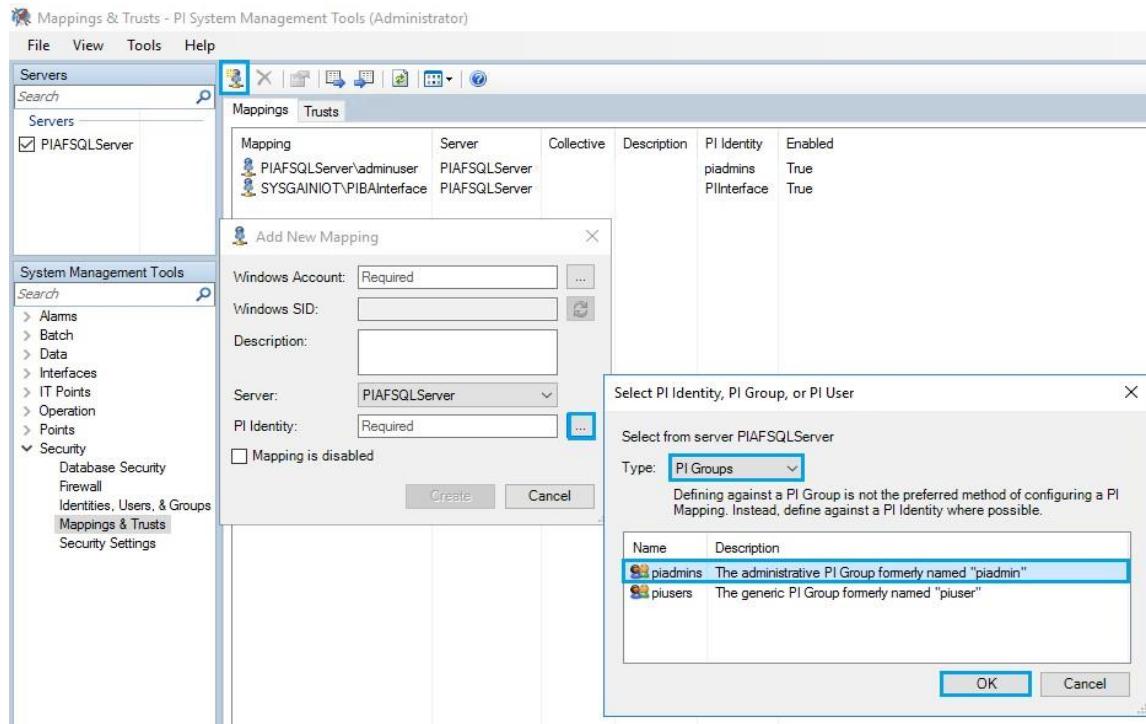
17. Under object name, type adminuser and click on **Check Names**, the following value **PIAFSQLServer\adminuser** will be populated automatically. Click on **OK**.



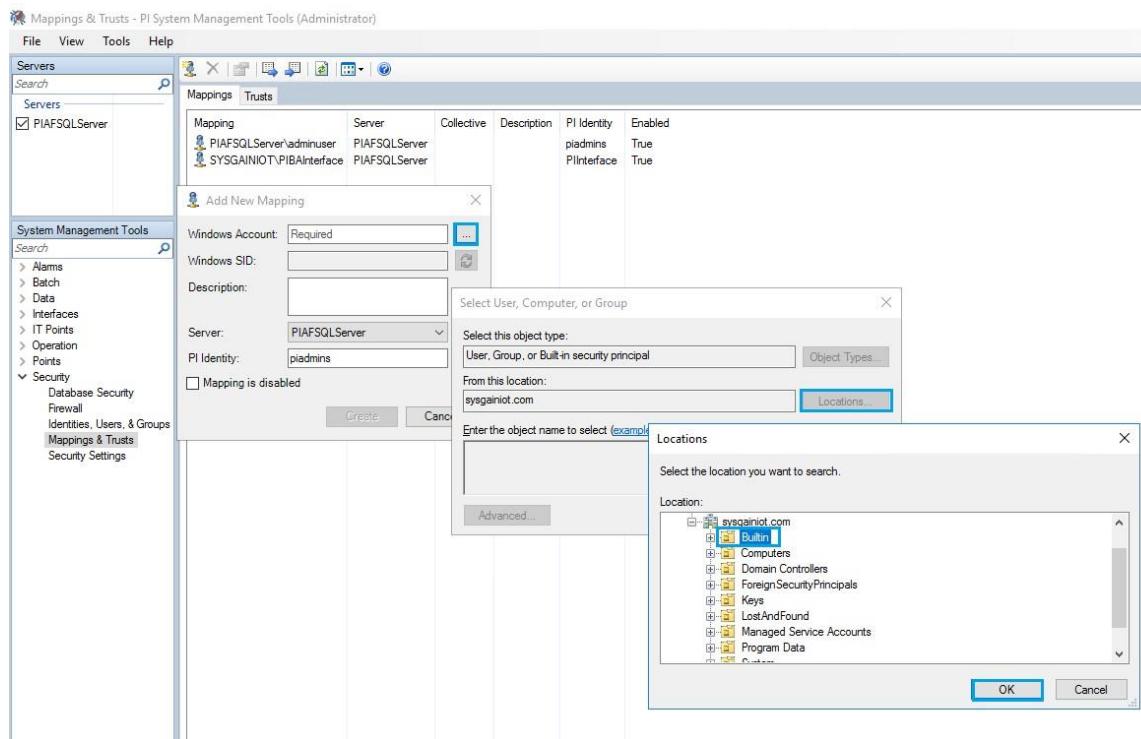
18. Click on **Create**



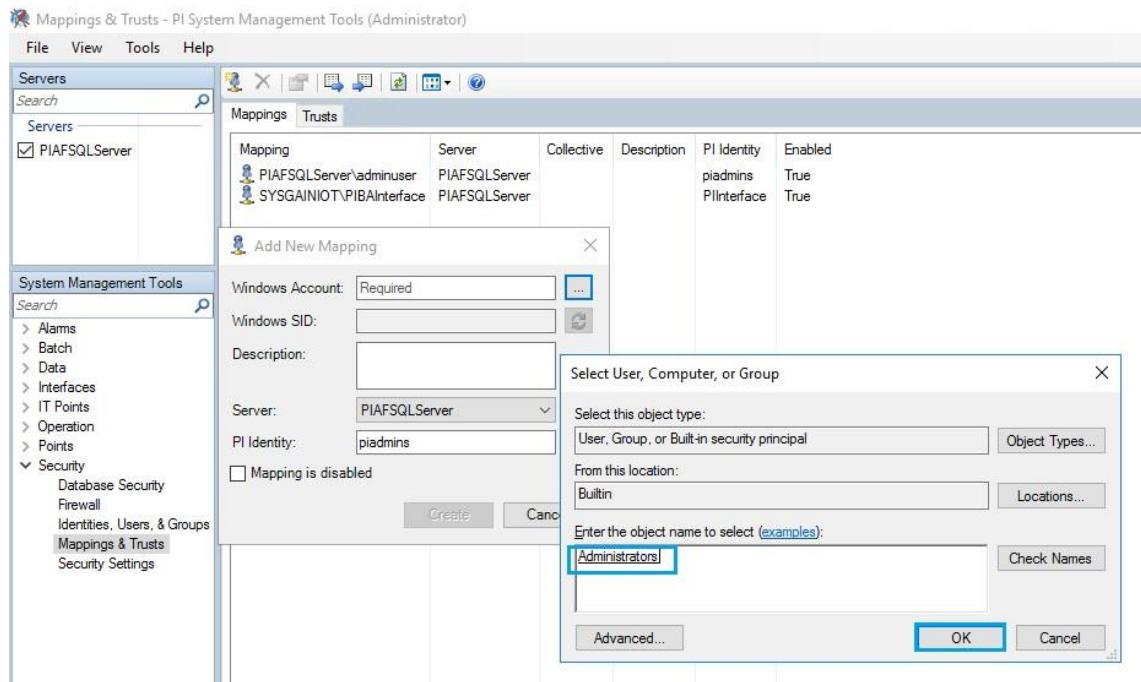
19. Create a new Mapping for **Administrator**. Click on the Mappings above symbol to add new mapping
20. Browse **PI Identity** end, select **Type as PI Groups** > Select **piadmins** > Click on **OK**.



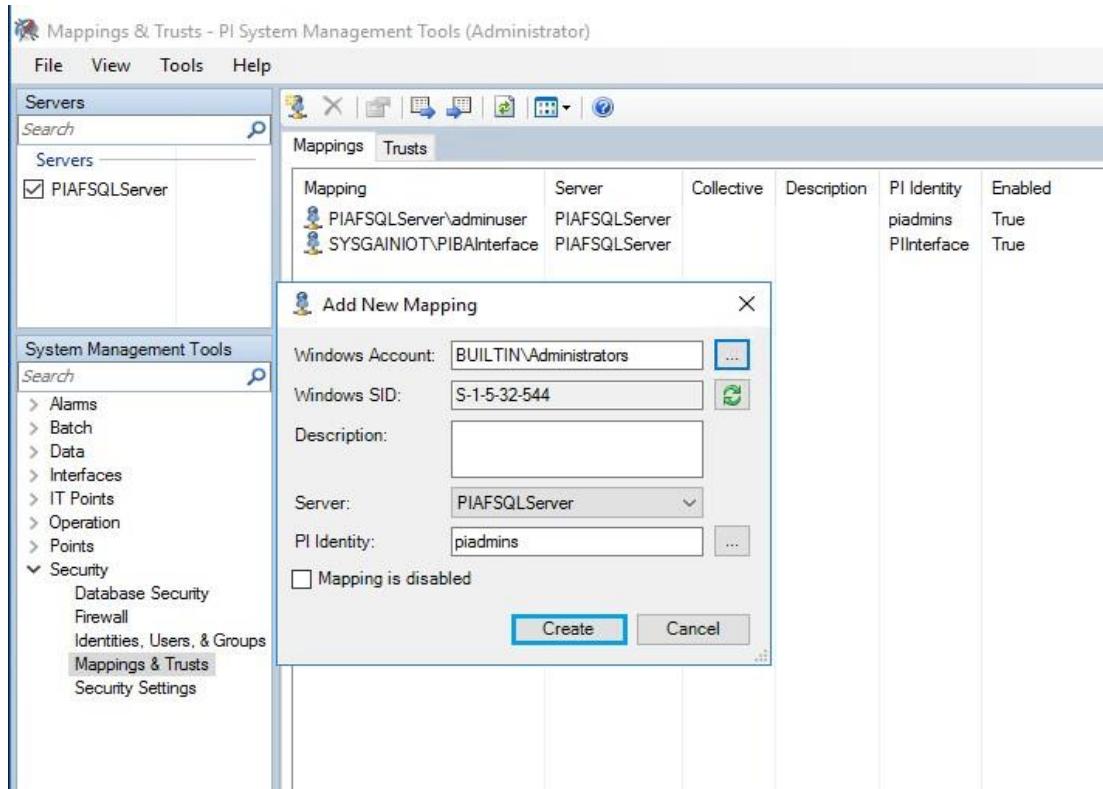
21. Click the Browse dots near **Windows Account** > Select **Locations** > click on **sysgaineriot.com** > Select **Builtin** > Click **OK**.



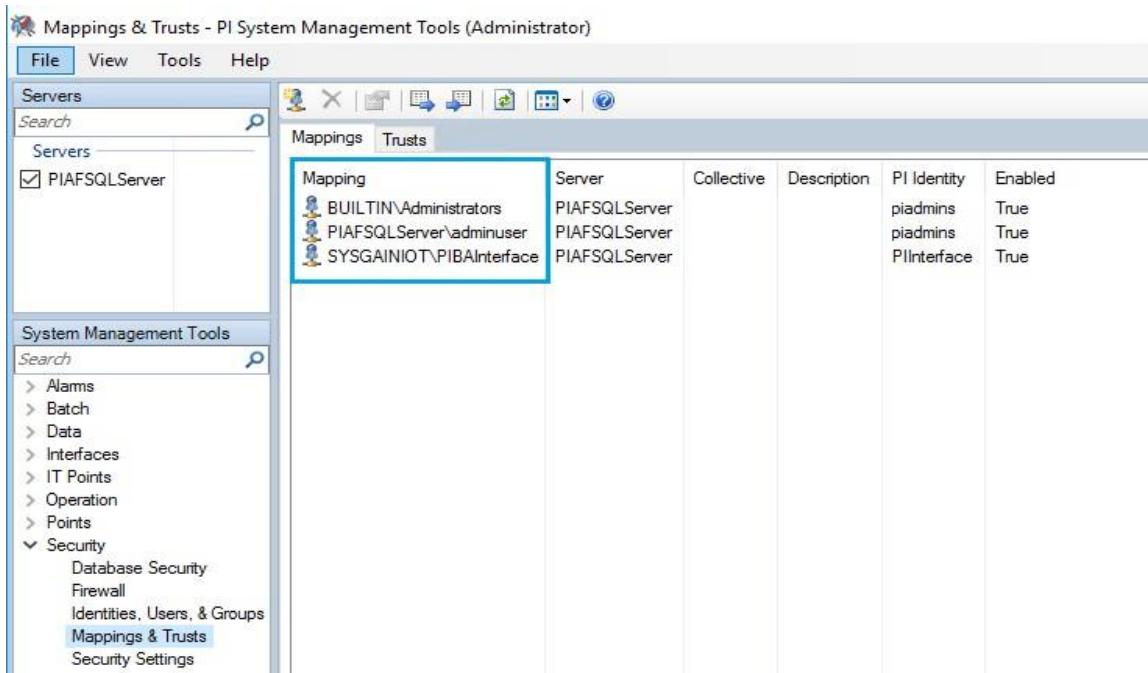
22. Enter the object name as **Administrators**, click on **Check Names** and click on **OK**.



23. Click on **Create**.

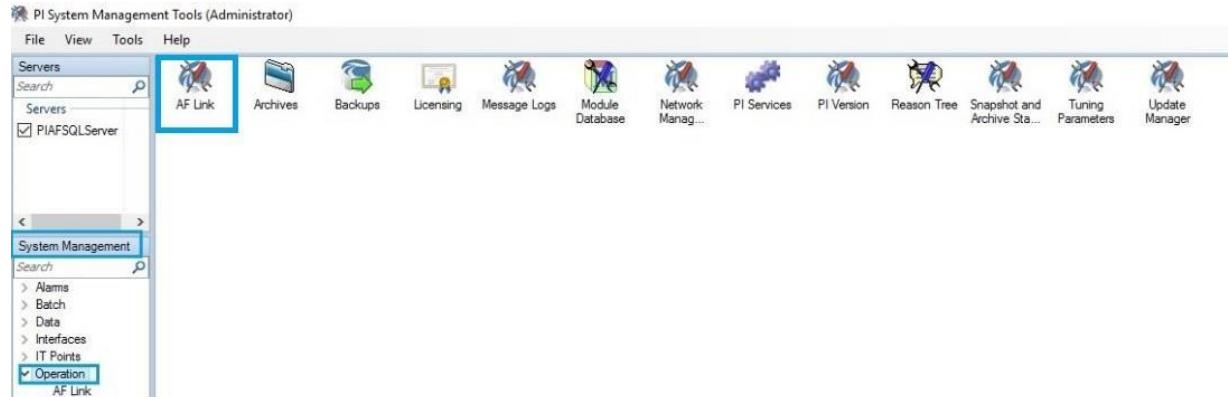


24. Verify the list of Mappings created.

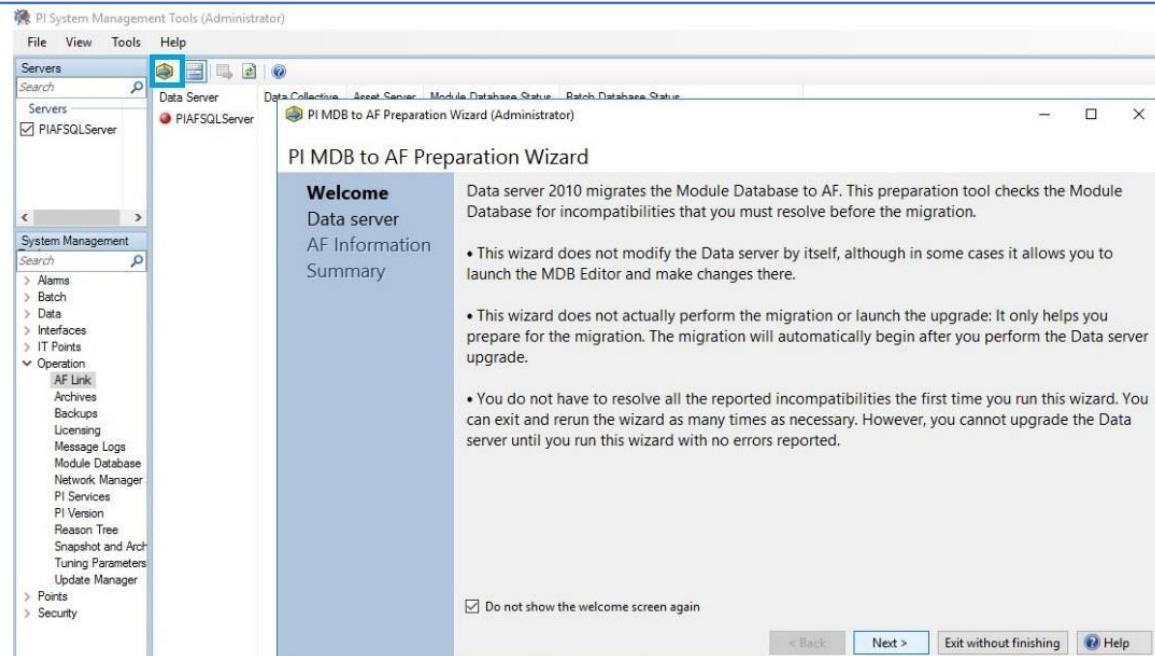


9.8. Prepare Data Server for Module Database(MDB) To Asset Framework(AF)

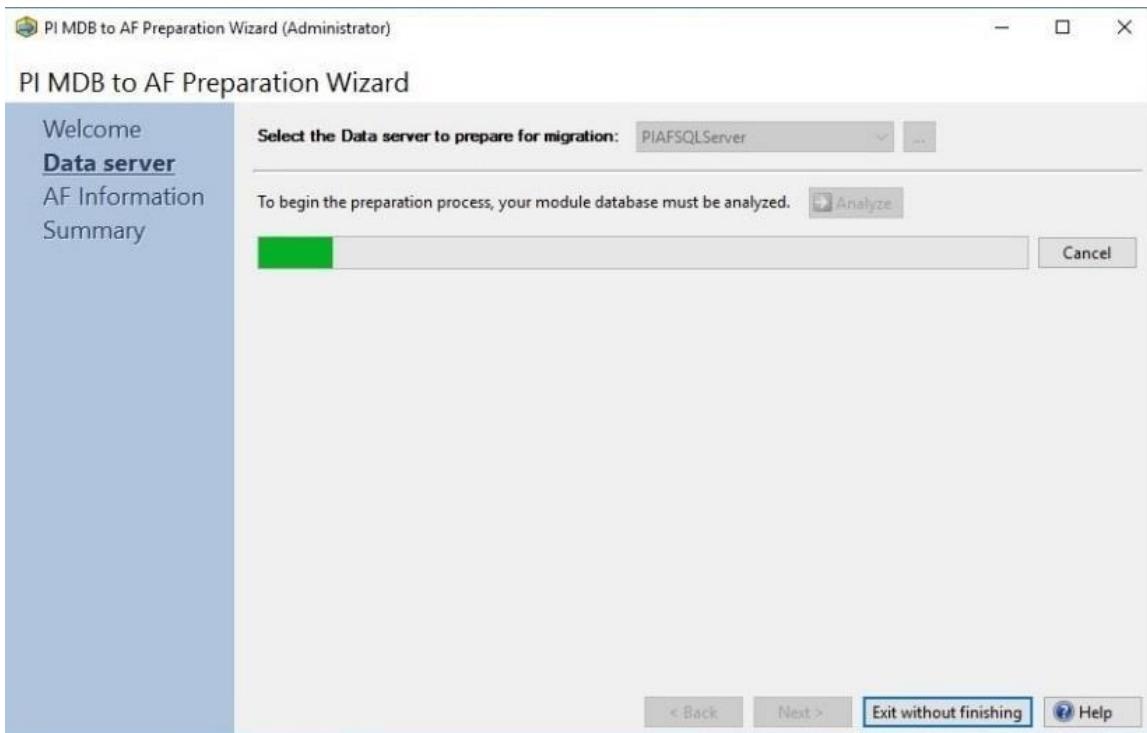
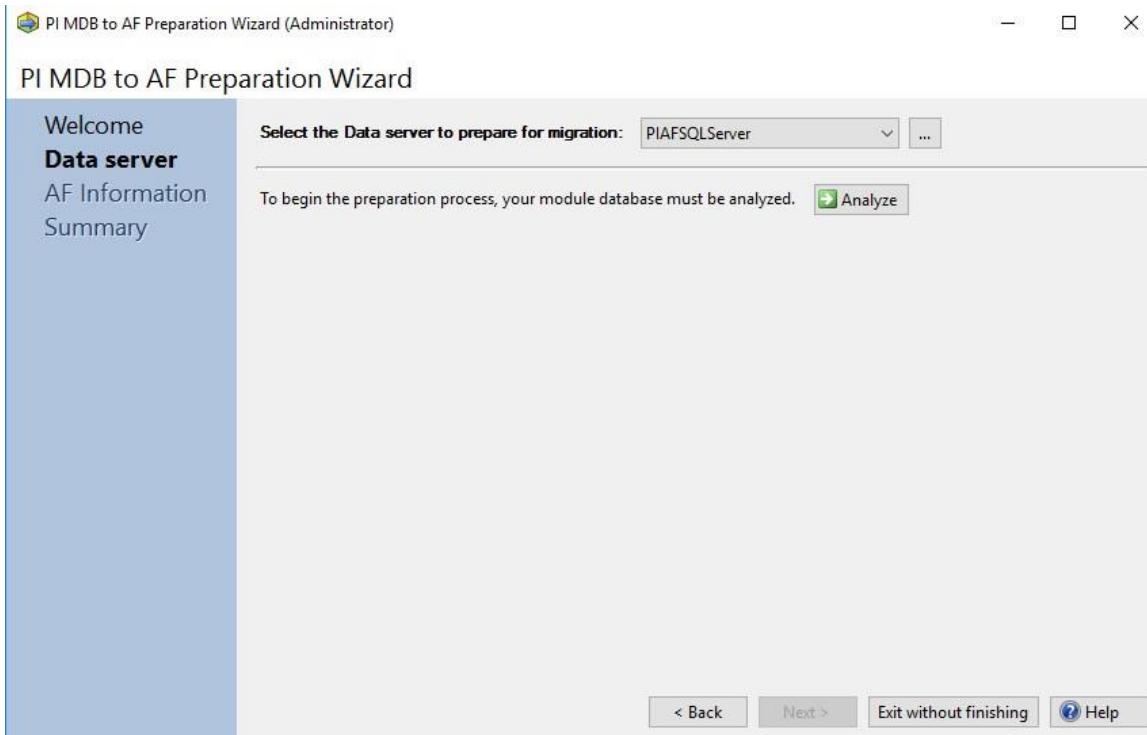
1. Navigate to **PI System Management Tools > Operation > Click on AF link.**



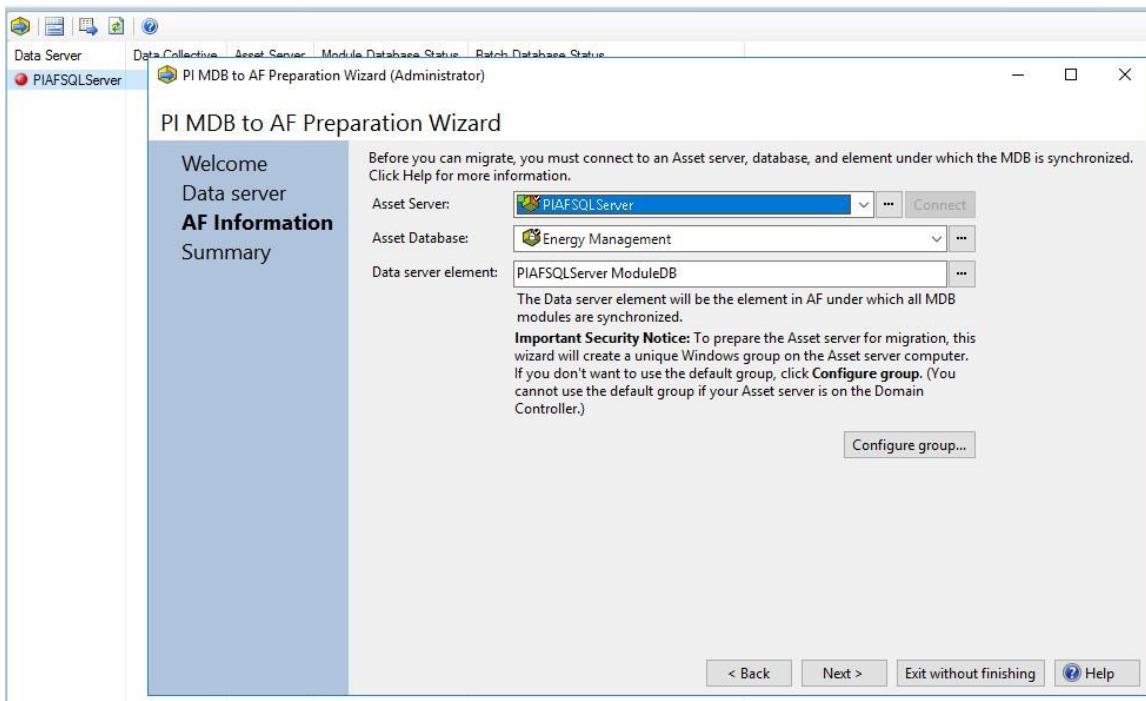
2. Click on **MDB to AF synchronization Wizard** (the symbol just below the **Help** tab). It will open the PI MDB to AF Preparation Wizard as shown below. Tick the do not show the welcome screen again checkbox ,Click on **Next**.



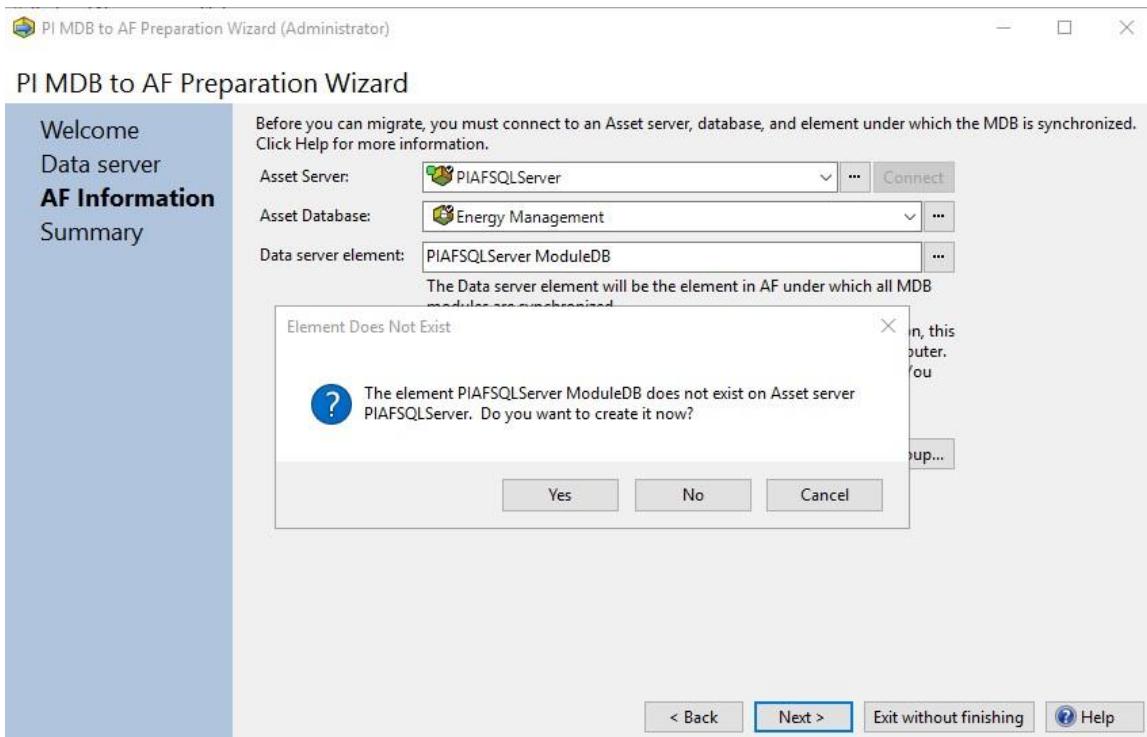
3. Click on **Analyze**, then click on **Next** and again click on **Next** once the process is complete.



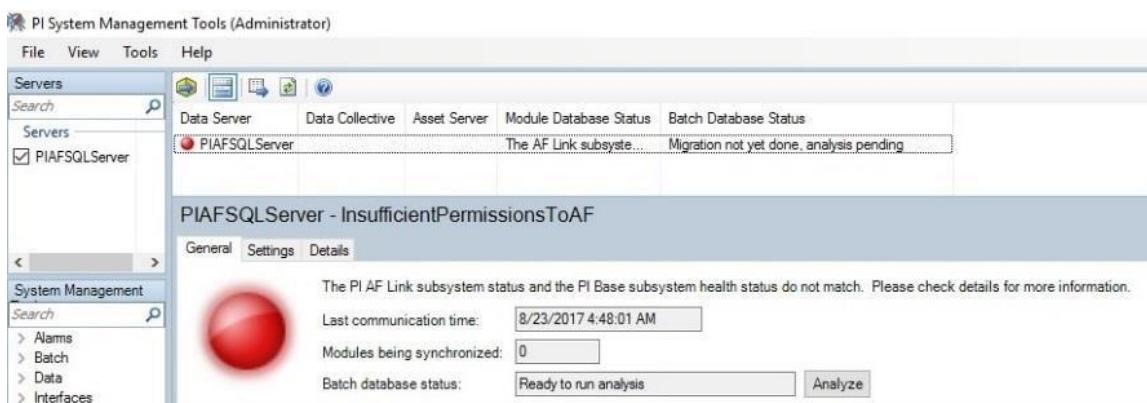
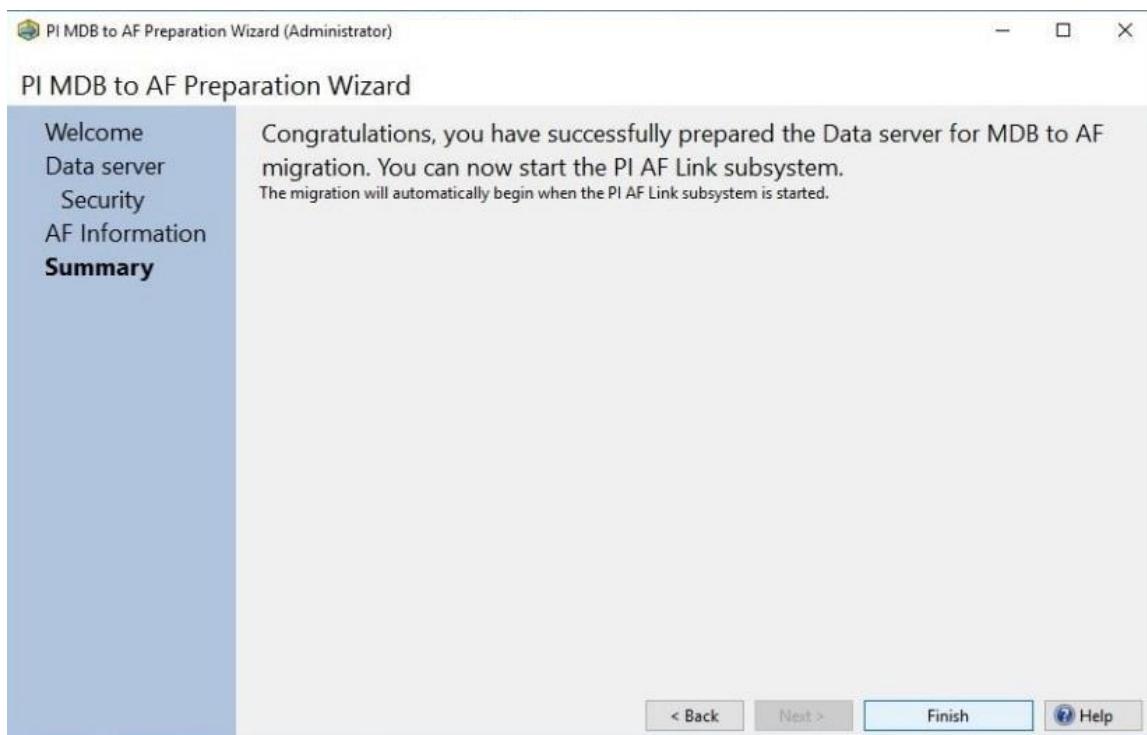
4. In AF Information, set the **Asset Server** as **PIAFSQLServer**, then click on **Connect**. Set **Asset Database** as **Energy Management**. Click on **Next**.



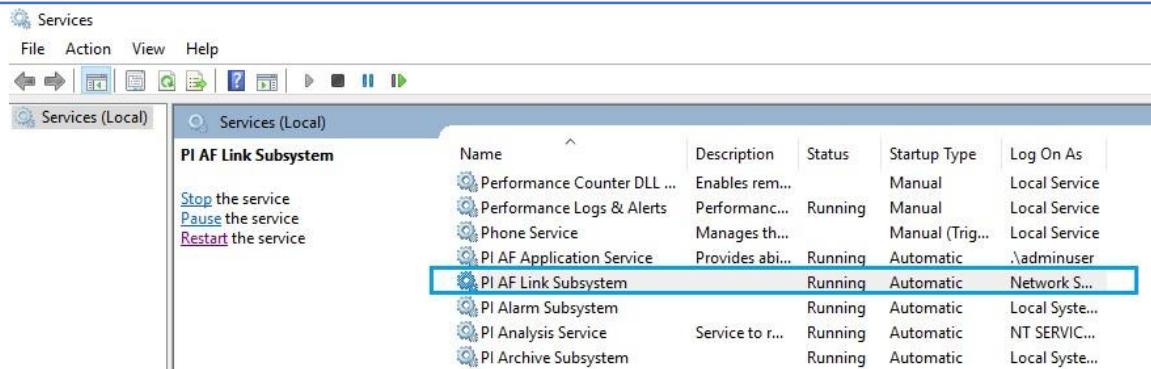
5. Click on **Yes** to create a PIAFSQLServer ModuleDB, then click on **Next**.



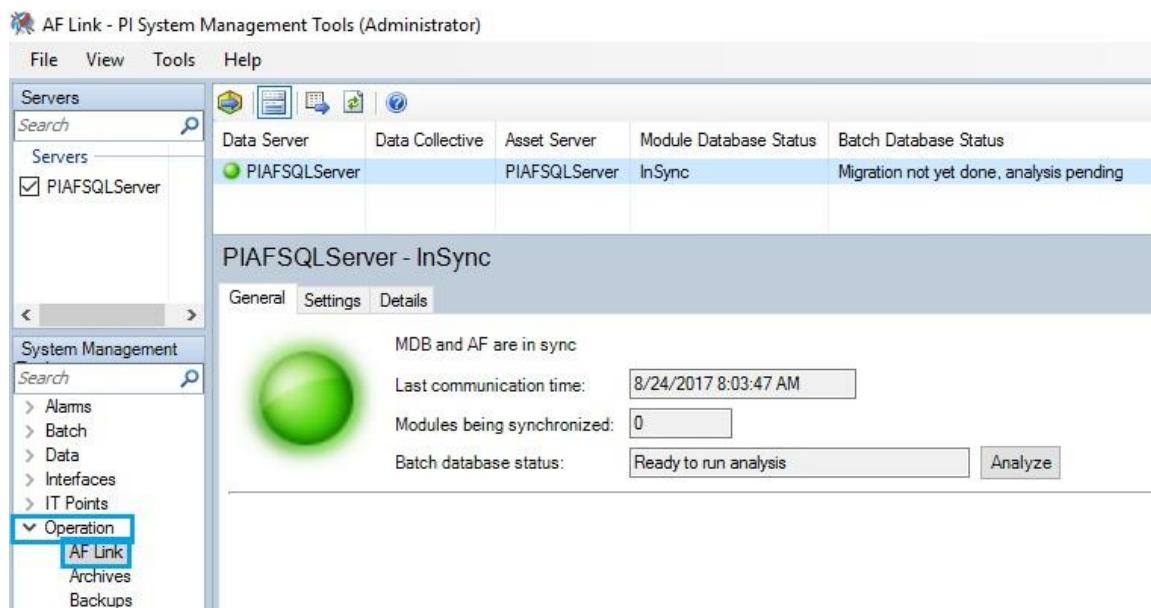
6. Click on **Finish**.



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



- 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 P371602028

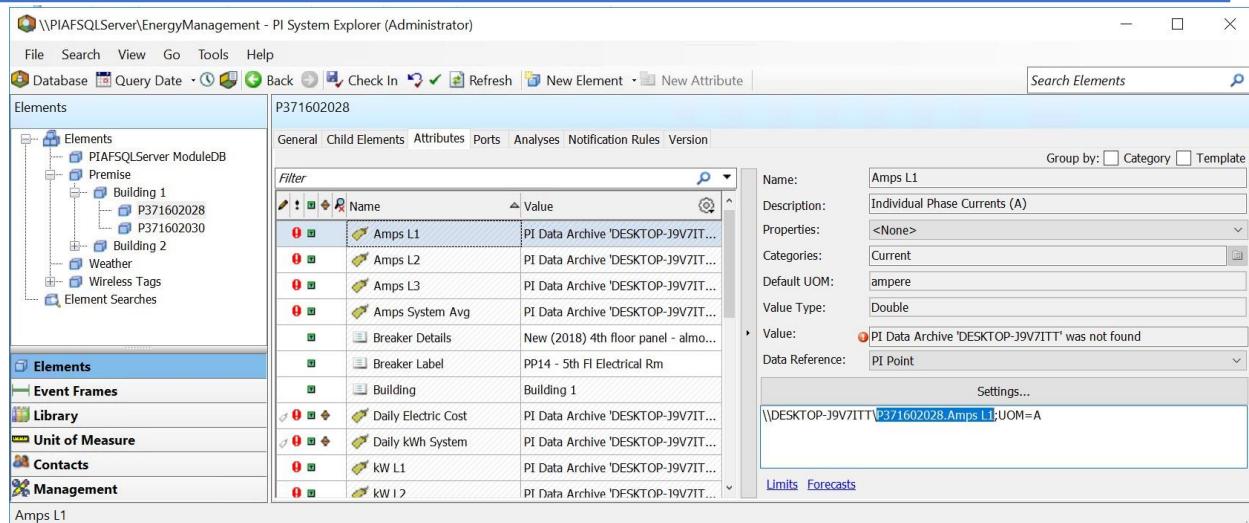
General	Child Elements	Attributes	Ports	Analyses	Notification Rules	Version
Filter						
<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
		Name		Value		
!		Amps L1		PI Data Archive 'DESKTOP-J9V7ITT' 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		

- To update the attribute, click on a **Name**. Then, under Settings, copy the PI point as shown below.

For example1, \\DESKTOP-J9V7ITT\\P371602028.Amps L1;UOM=A the highlighted part (the text between “\\” and “;”).

For exxample2, \\DESKTOP-J9V7ITT\\P371602028.Daily Electric Cost.60e6094f-e554-5e8f-1742-54def61fbe81

In such cases copy full point after “ \\ ”



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

File View Tools Help

Servers

Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor

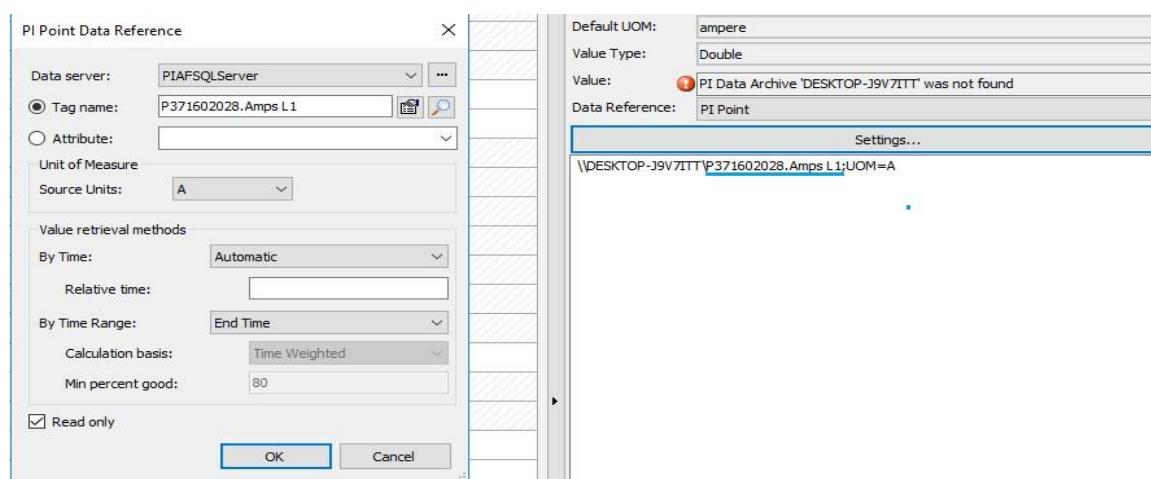
System Management Tools

General	Archive	Classic	Security	System
Name: P371602028.Amps L1				
Descriptor: P371602028.Amps L1				
Stored Values: Real-time data	Point Source:	Modbus		
Point Type: Float64	Digital Set:			
Eng Units:				
Exdesc:				
Source Tag:				

Session Record

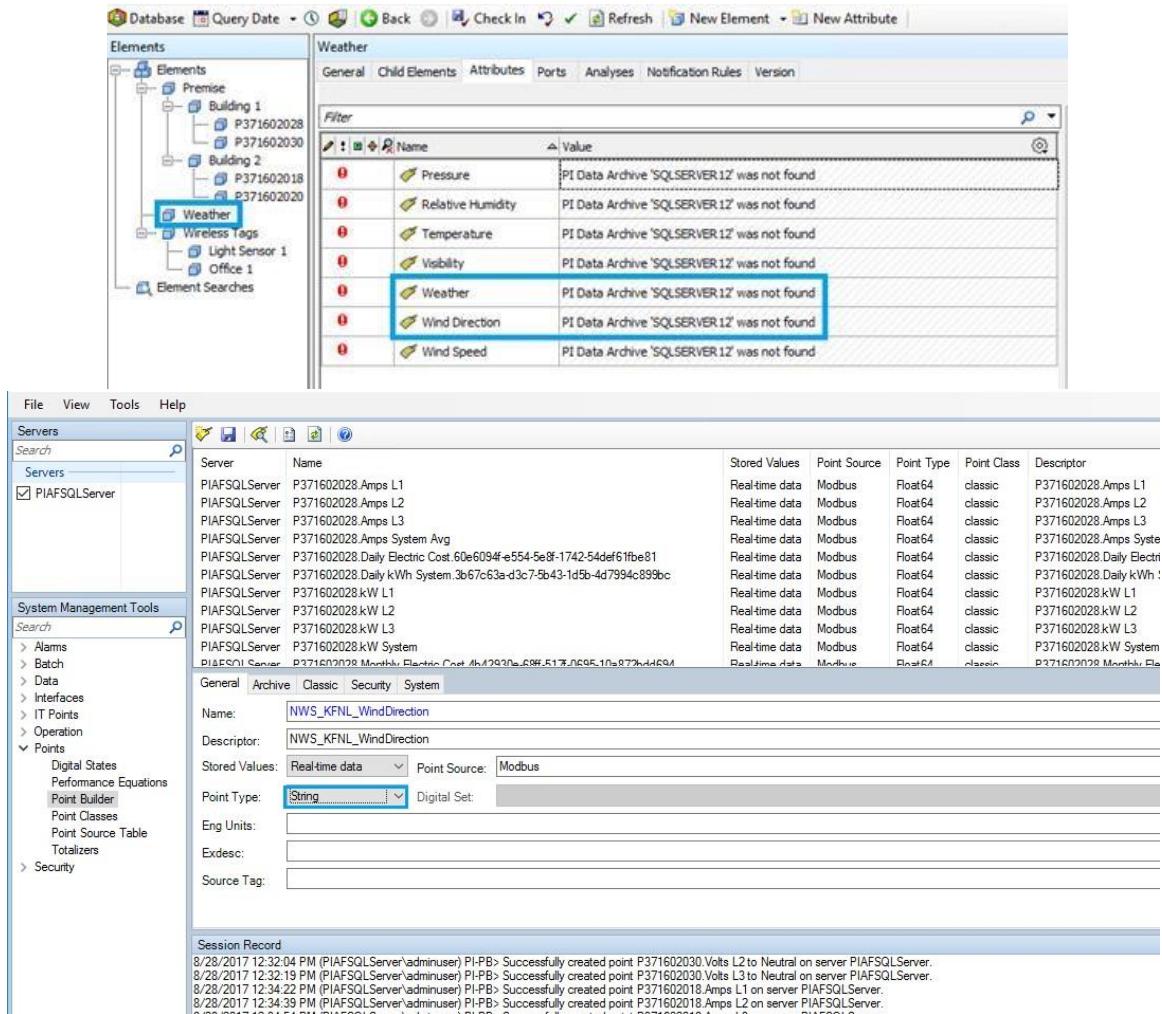
```
8/28/2017 10:43:54 AM (PIAFSQLServer\adminuser) PI-IUGE> Edited Identity PIWorld.
8/28/2017 10:46:20 AM (PIAFSQLServer\adminuser) PI-IUGE> Added identity 'PIInterface' to server 'PIAFSQLServer'.
8/28/2017 10:58:16 AM (PIAFSQLServer\adminuser) PI-IUGE> Edited Identity PIInterface.
```

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.



The screenshot shows the PI System Database interface. On the left, the 'Elements' tree view shows a 'Weather' node under 'Building 1'. On the right, the 'Weather' tab of the 'General' pane is selected, displaying a table of points. The 'Wind Direction' and 'Weather' rows are highlighted with a blue border. In the bottom-right pane, the 'System Management Tools' section is open, specifically the 'Points' tab. Under 'General' settings for the 'NWS_KFNL_WindDirection' point, the 'Point Type' dropdown is set to 'String'. The session record at the bottom shows successful creation of the point.

Name	Value
Pressure	PI Data Archive 'SQLSERVER12' was not found
Relative Humidity	PI Data Archive 'SQLSERVER12' was not found
Temperature	PI Data Archive 'SQLSERVER12' was not found
Visibility	PI Data Archive 'SQLSERVER12' was not found
Weather	PI Data Archive 'SQLSERVER12' was not found
Wind Direction	PI Data Archive 'SQLSERVER12' was not found
Wind Speed	PI Data Archive 'SQLSERVER12' was not found

Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor
PIAFSQLServer	P371602028.Amps L1	Real-time data	Modbus	Float64	classic	P371602028.Amps L1
PIAFSQLServer	P371602028.Amps L2	Real-time data	Modbus	Float64	classic	P371602028.Amps L2
PIAFSQLServer	P371602028.Amps L3	Real-time data	Modbus	Float64	classic	P371602028.Amps L3
PIAFSQLServer	P371602028.Amps System Avg	Real-time data	Modbus	Float64	classic	P371602028.Daily Electric
PIAFSQLServer	P371602028.Daily Electric Cost .60e6094-e554-5e8f-1742-54def6ffbe81	Real-time data	Modbus	Float64	classic	P371602028.Daily Electric
PIAFSQLServer	P371602028.Daily kWh System .3b67c63a-d3c7-5b43-1d5b-4d7994c899bc	Real-time data	Modbus	Float64	classic	P371602028.Daily kWh
PIAFSQLServer	P371602028.kW L1	Real-time data	Modbus	Float64	classic	P371602028.kW L1
PIAFSQLServer	P371602028.kW L2	Real-time data	Modbus	Float64	classic	P371602028.kW L2
PIAFSQLServer	P371602028.kW L3	Real-time data	Modbus	Float64	classic	P371602028.kW L3
PIAFSQLServer	P371602028.kW System	Real-time data	Modbus	Float64	classic	P371602028.kW System
PIAFSQLServer	P371602028.Monthly_Electric_Cost_MhA7Q2028.C9F_E13_0C05_10a277A4H9A	Real-time data	Modbus	Float64	classic	P371602028.Monthly_Electric_Cost_MhA7Q2028.C9F_E13_0C05_10a277A4H9A

9.10. Install and Run The Piweb Simulator Setup

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

Settings

 Home

Some settings are managed by your organization.

Find a setting 

Time & language

Date and time

 Date & time

Set time automatically

 On Region & language

Set time zone automatically

 Off SpeechChange 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)

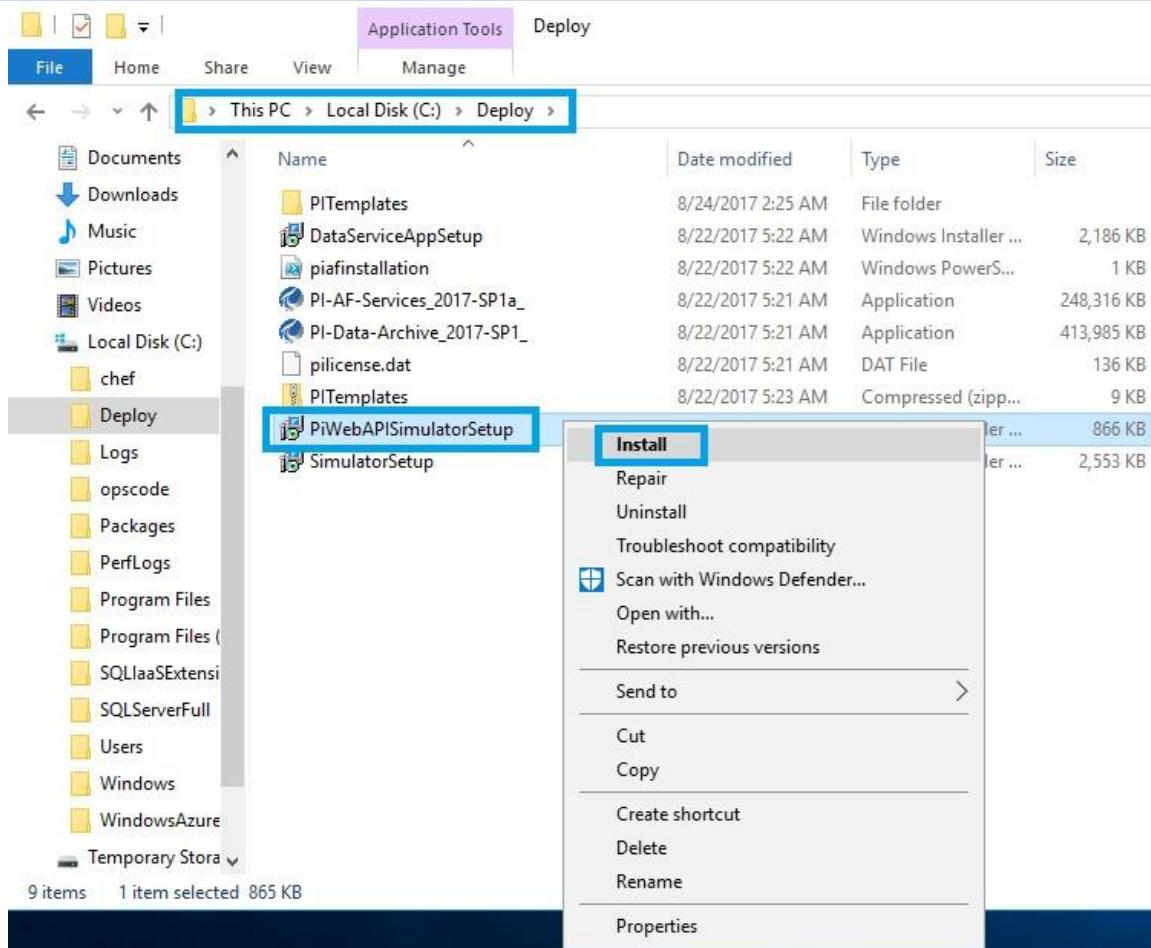
(UTC-06:00) Easter Island

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

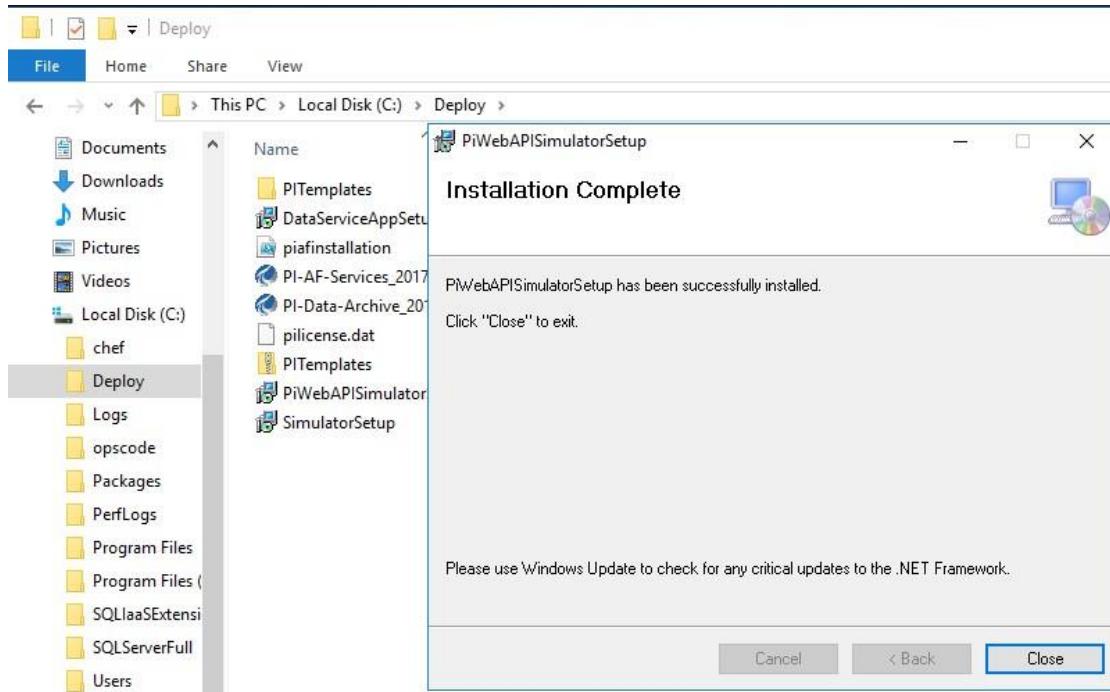
First day of week: Sunday

Short date: 8/24/2017

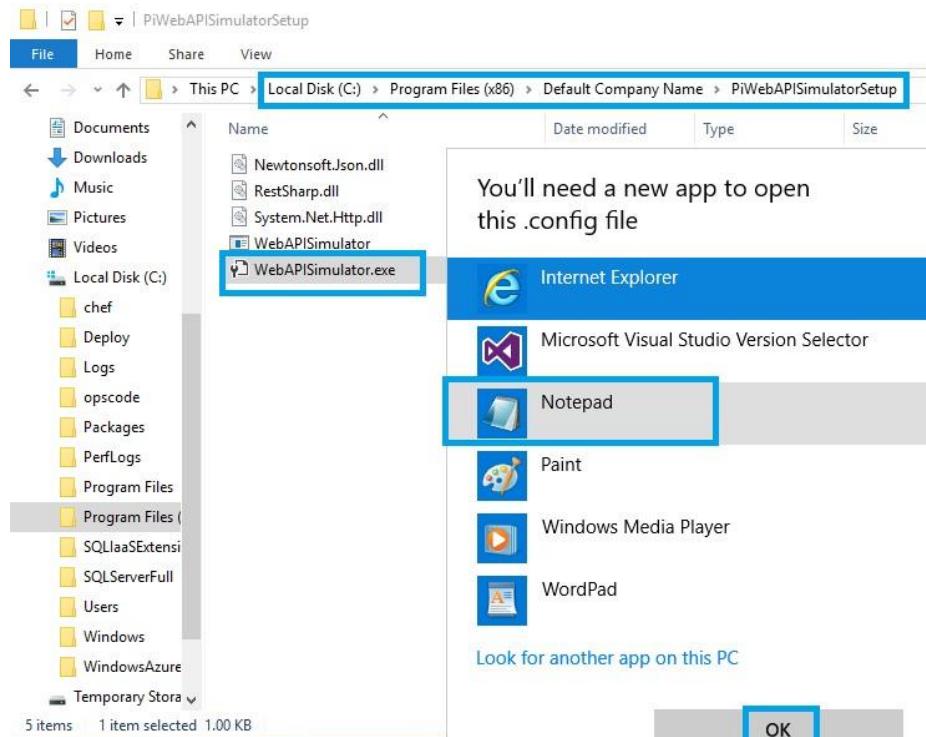
2. Navigate to the **Local Disk (C:) > Deploy > PIWebAPISimulatorSetup** and right-click to **Install**.



- 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**.



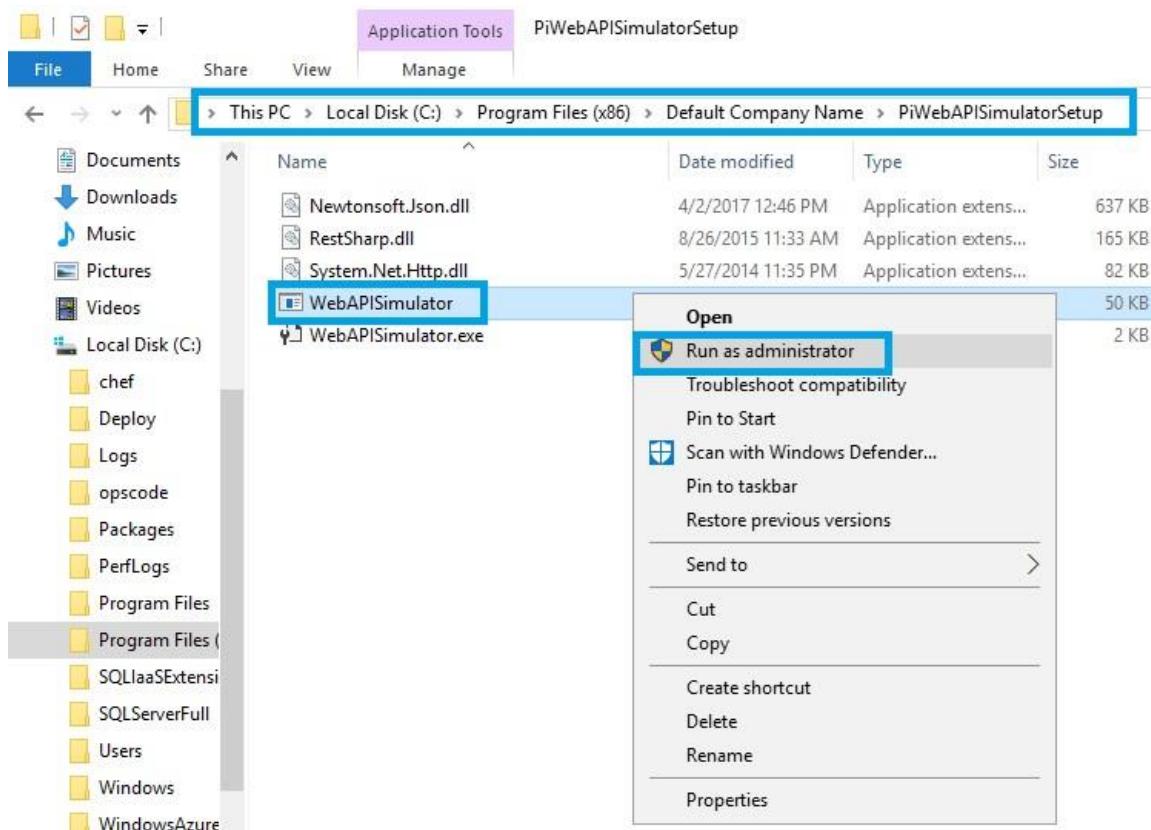
The screenshot shows a Notepad window titled "WebAPISimulator.exe - Notepad". The content is an XML configuration file. A blue rectangular box highlights the `<appSettings>` section, which contains the app settings defined in the previous code block. The entire file is as follows:

```

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <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"/>

    <add key="TimeStarter" value="0"/>
  </appSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>
```

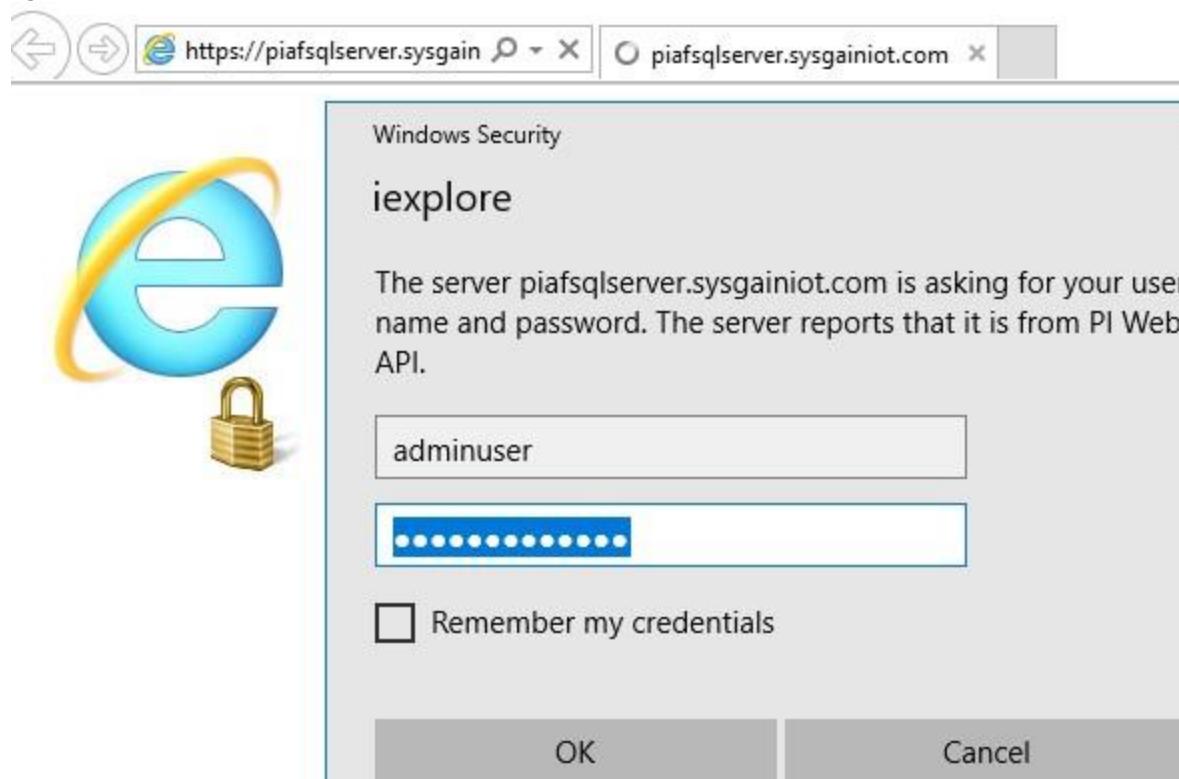
6. Navigate to **Local Disk (C:) > Program Files(X86) > Default Company Name > PiwebAPISimulatorSetup**. Select the **WebAPISimulator**, right click to **Run as Administrator**.



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

```
Select C:\Program Files (x86)\Default Company Name\PiWebAPISimulatorSetup\WebAPISimulator.exe
*****
Response created *****
Completed Status code is: Accepted
Status Description: Accepted
Done with processing of building :: Building 1
for powerscout P371602018
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzz2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
***** Response created *****
Completed Status code is: Accepted
Status Description: Accepted
for powerscout P371602018
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzz2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
***** 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 c3lzz2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
***** Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzz2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
***** 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
```

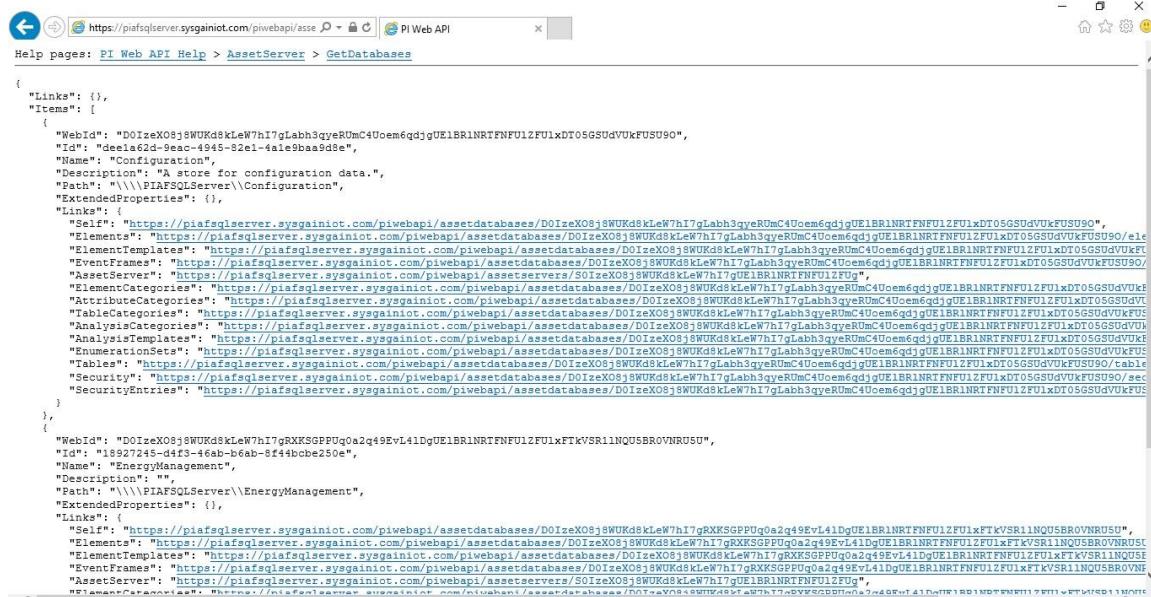
- Paste the URL <https://piafsqlserver.sysgainiot.com/piwebapi/> in **Internet Explorer** to view the Data servers URLs. It will show a popup box like below. Enter PIAFSQLServer credentials to login.



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



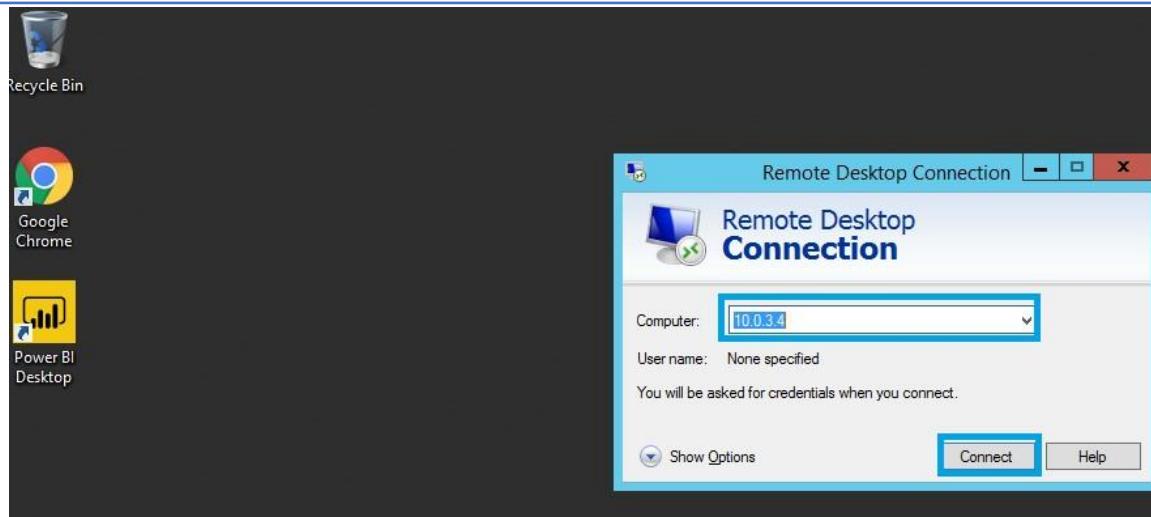
```

{
  "Links": {},
  "Items": [
    {
      "WebId": "DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90",
      "Id": "de1a2d-9eac-4945-82e1-4a1e9baa5d8",
      "Name": "Configuration",
      "Description": "A store for configuration data.",
      "Path": "\\\\PIAFSQLserver\\Configuration",
      "ExtendedProperties": {}
    },
    {
      "Links": {
        "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90",
        "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/elements",
        "ElementTemplates": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/elementTemplates",
        "EventFrames": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/eventFrames",
        "AssetServer": "https://piafsqlserver.sysgainiot.com/piwebapi/assetServers/SOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90",
        "AssetCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/assetCategories",
        "Actions": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/actions",
        "AnalysisCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/analysisCategories",
        "AnalysisTemplates": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/analysisTemplates",
        "EnumerationSets": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/enumerationSets",
        "Tables": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/tables",
        "Security": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/security",
        "SecurityEntries": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gLabh3qyeRUMC4Uoem6qdjgUE1BR1NRTNFNU1ZFU1xDT05GSUdVUkFUSU90/securityEntries"
      }
    },
    {
      "WebId": "DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
      "Id": "18927245-d4f3-46ab-b6ab-8f4bce250e",
      "Name": "EnergyManagement",
      "Description": "",
      "Path": "\\\\PIAFSQLserver\\EnergyManagement",
      "ExtendedProperties": {},
      "Links": {
        "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
        "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
        "ElementTemplates": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
        "EventFrames": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
        "AssetServer": "https://piafsqlserver.sysgainiot.com/piwebapi/assetServers/SOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5",
        "AssetCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DOIzeXO8j8WUKd8kLeW7h17gRXKSGPPUq0a2q49EvL41dgUE1BR1NRTNFNU1ZFU1xFTkVSR11NQUSBROVRNRSU5"
      }
    }
  ]
}

```

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**

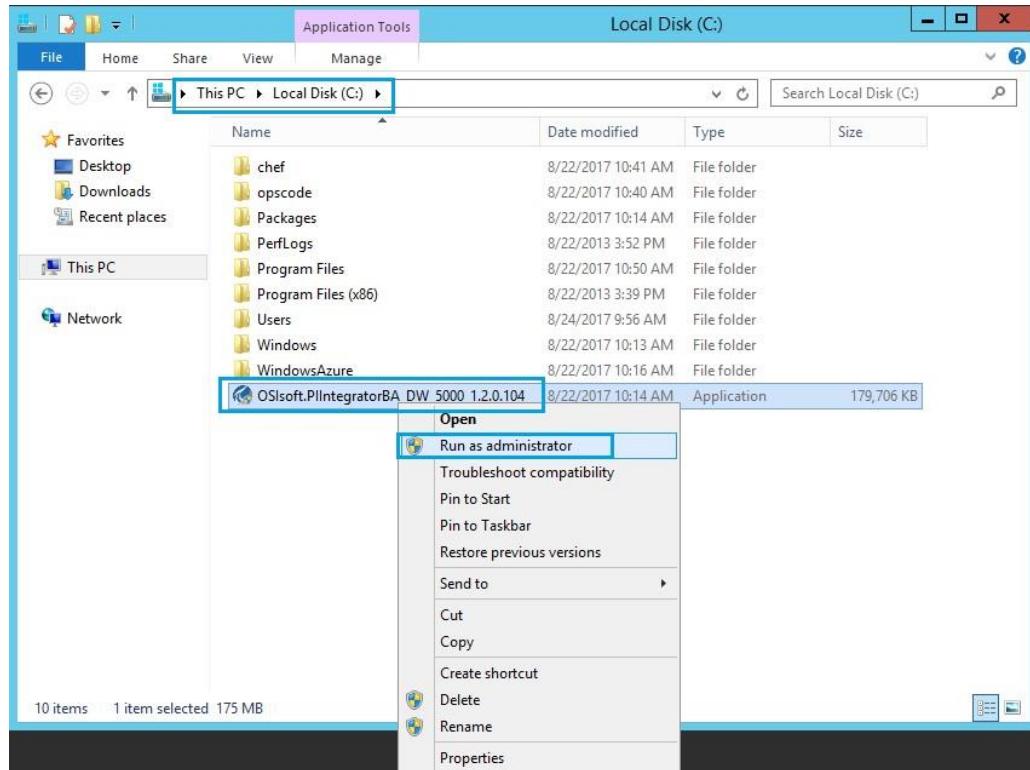


Note: Login with the **same** user credentials you created in the **ADServer**

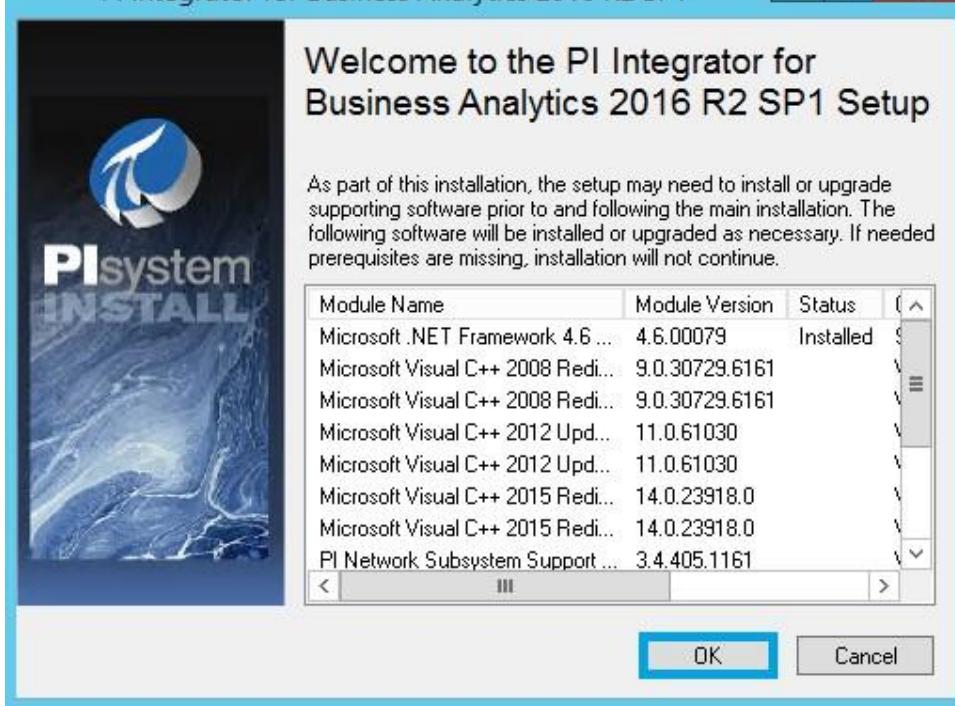
2. Login with credentials "**<domainname>\PIBAInterface**" (user you created in AD server) and **aq21password**.



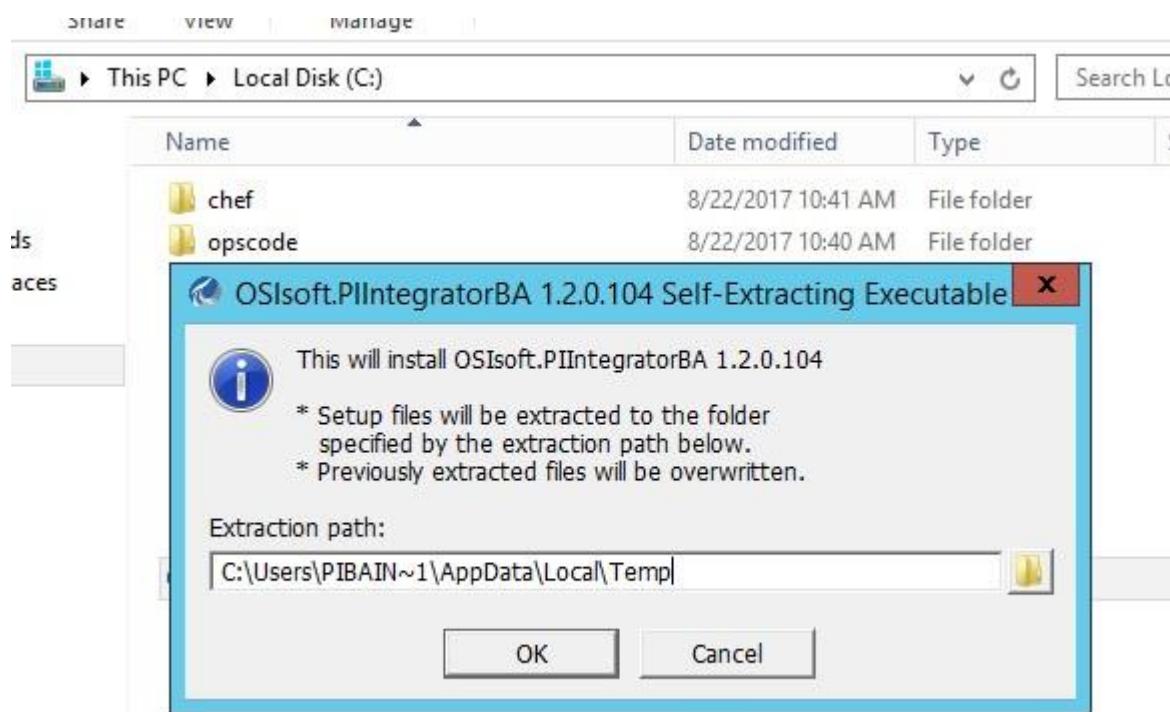
3. After connecting to the PIBA VMServer, navigate to the LocalDisk (C:) and select **OSISoft.PIIntegratorBA**, then right-click on and **Run as administrator**.



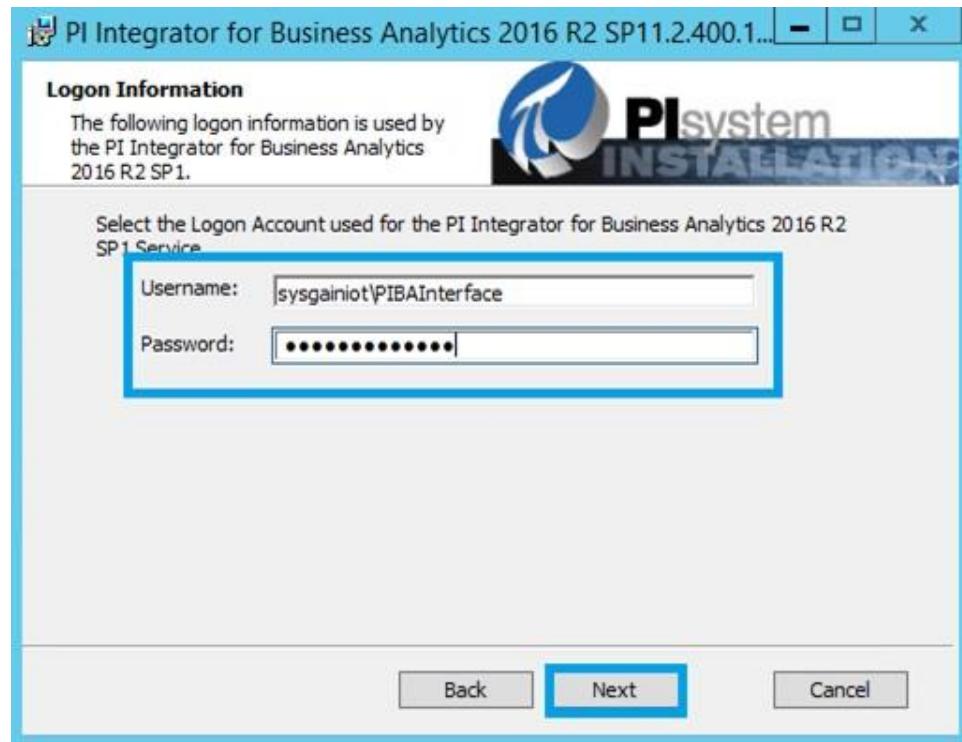
4. Click on **Ok**.



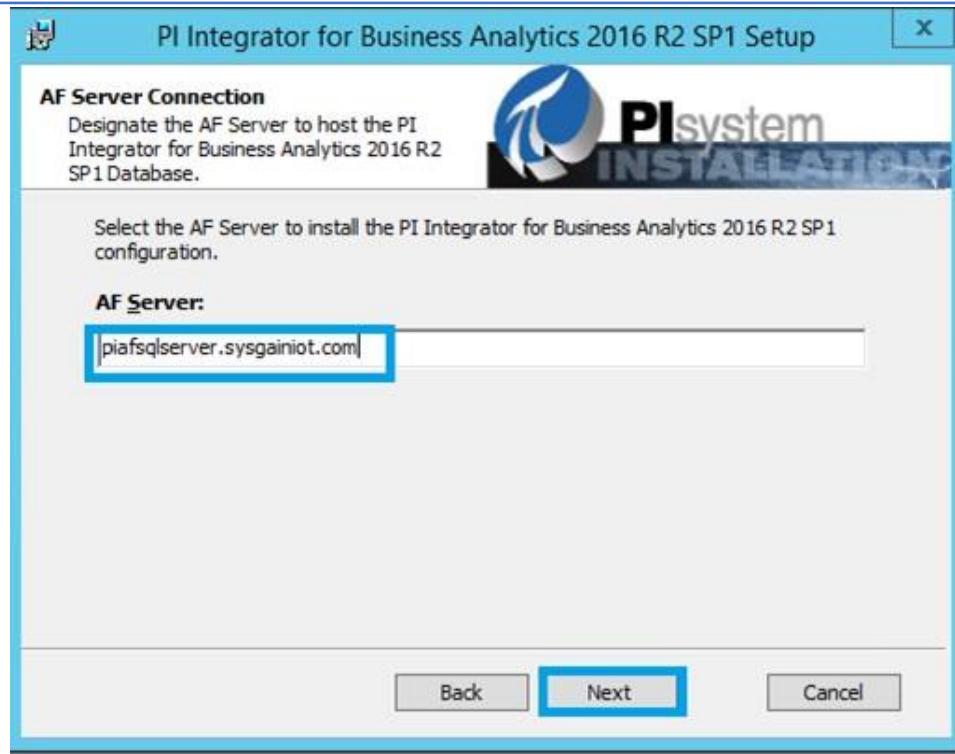
5. Click on **OK**



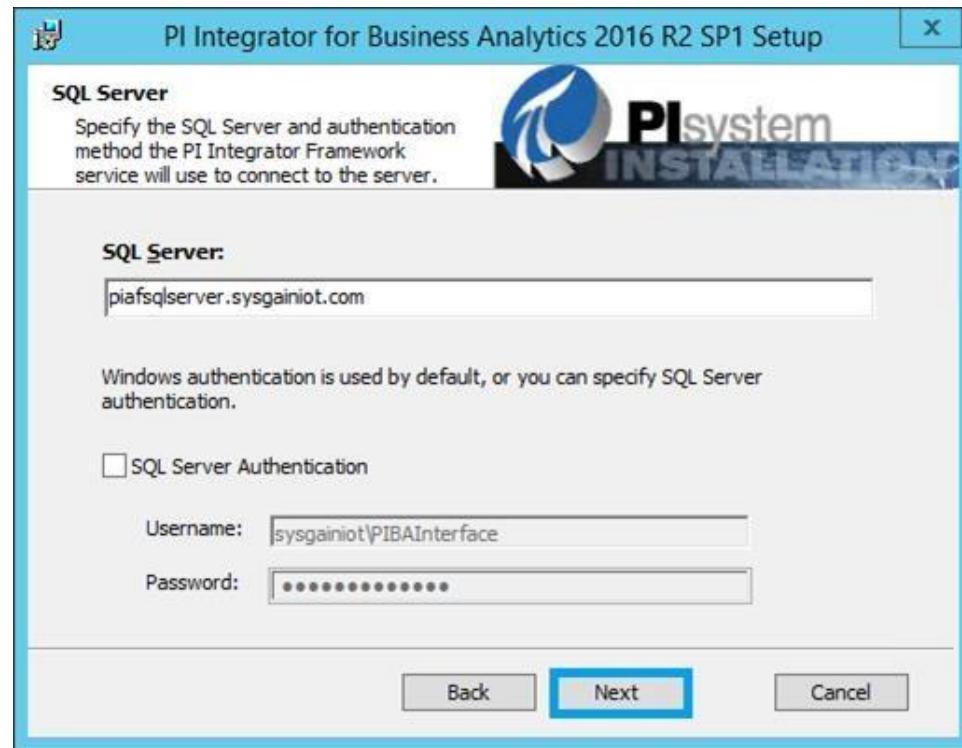
6. Give the same credentials which you used to login to PIBA server in Logon credentials and click on **Next**



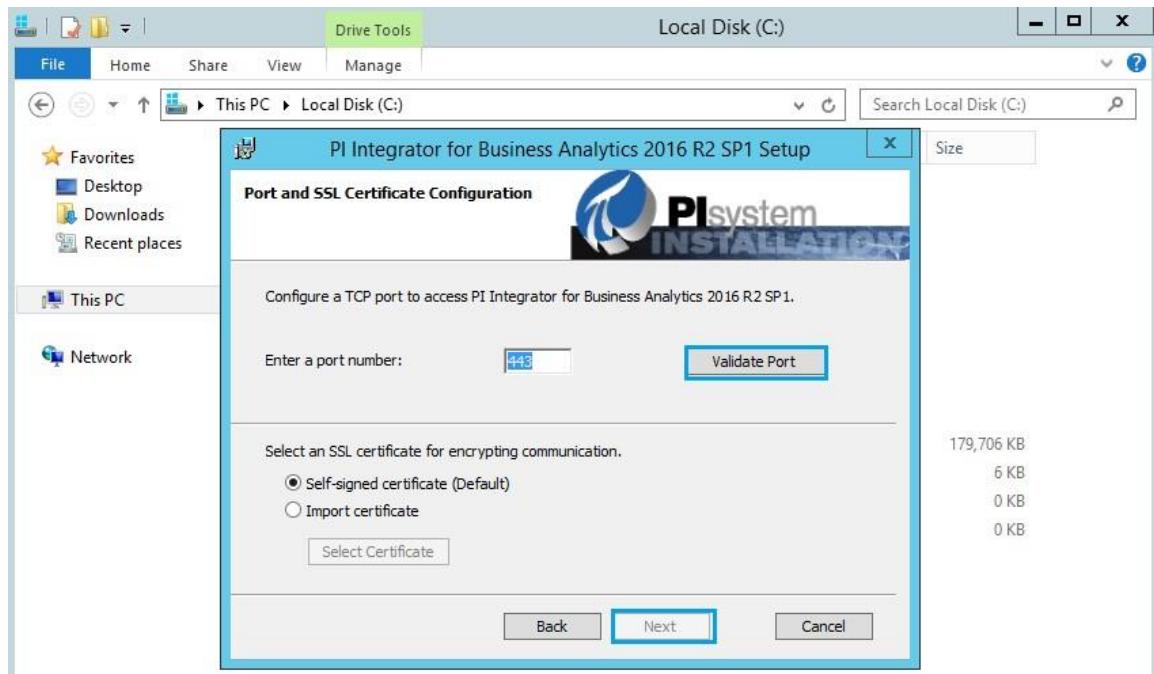
7. Give the AF sever link as piafsqlserver. <domainname> to host PIBA database and click on **Next**



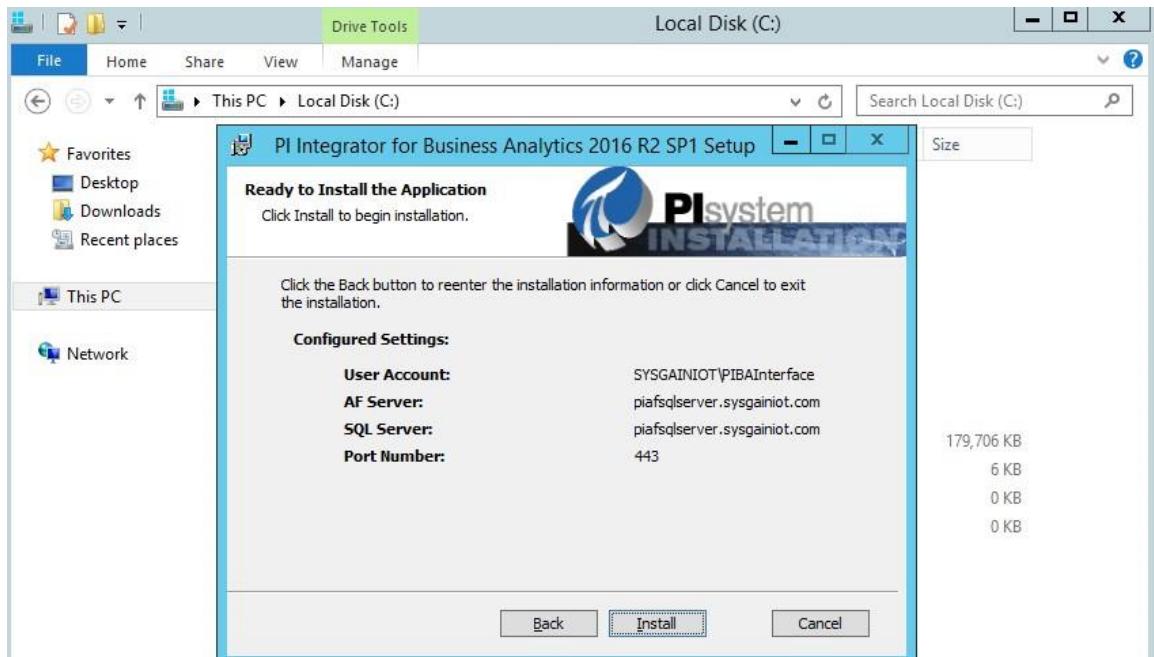
8. Click on **Next**



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

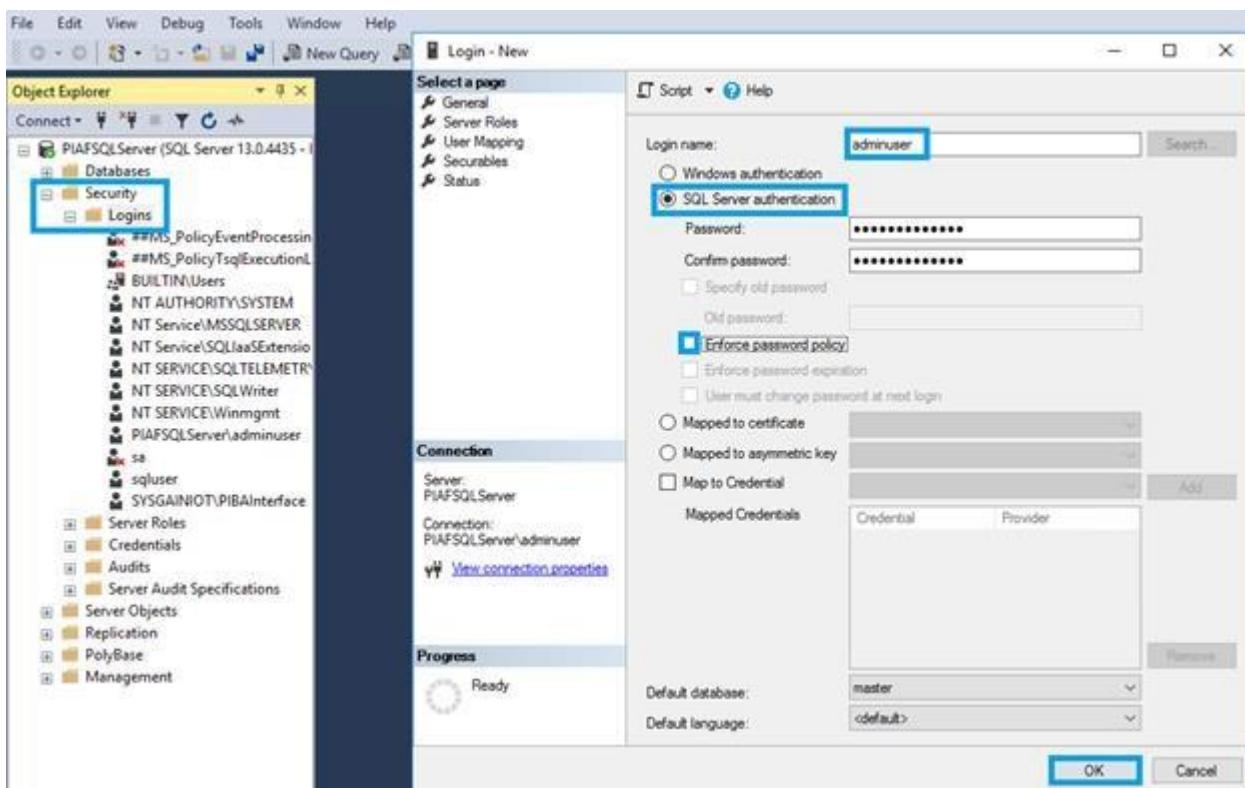


10. Click on **Install**.

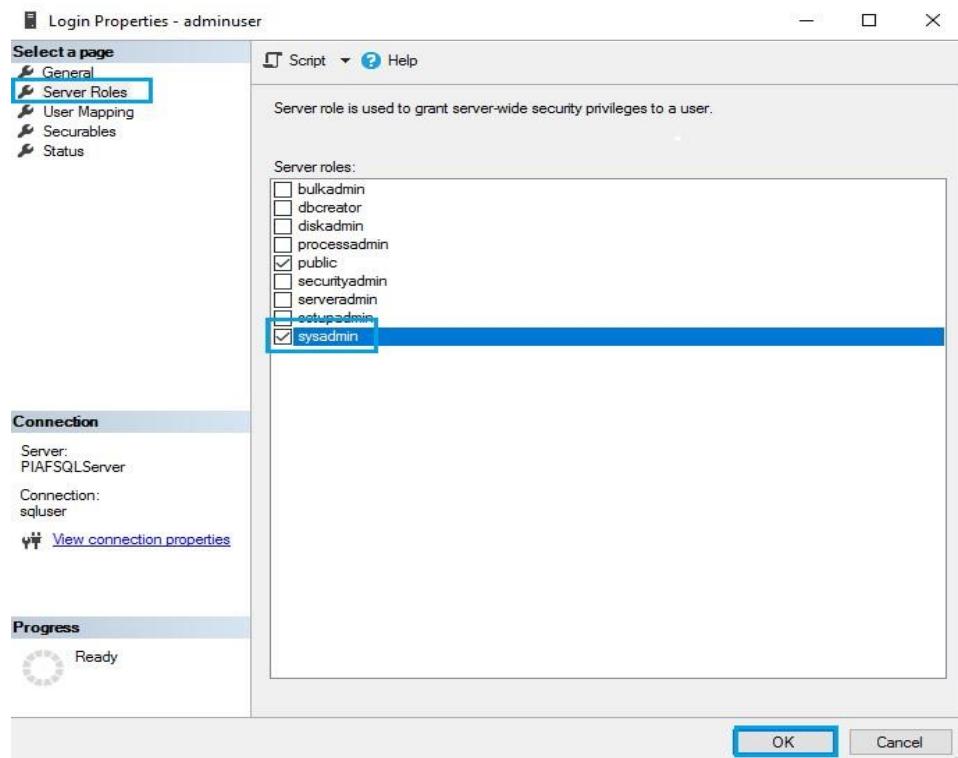


10.1. Configuring PI Business Analytics

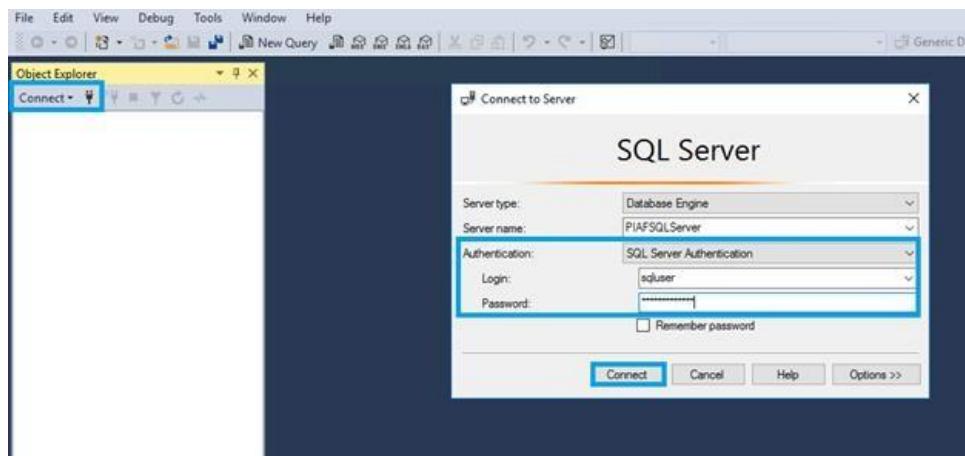
1. In Bastion Server, connect to the PIAFSQLServer with the credentials provided in the output section.
2. Go to the **Security** section, then right-click on **Login** and select **New Login**. Set the login name as **adminuser** and select **SQL Server Authentication**. Set a password and uncheck the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



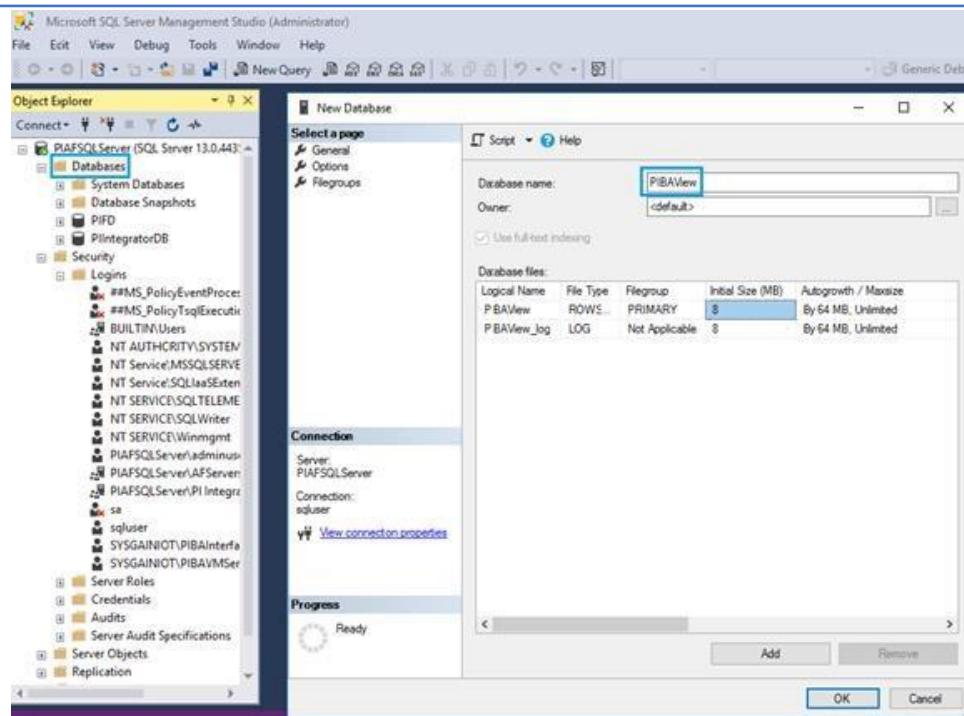
3. Right-click on the admin user under **Login** and select **Properties**. On the Properties screen, select **Server Roles**, then check **sysadmin** and click **Ok**.



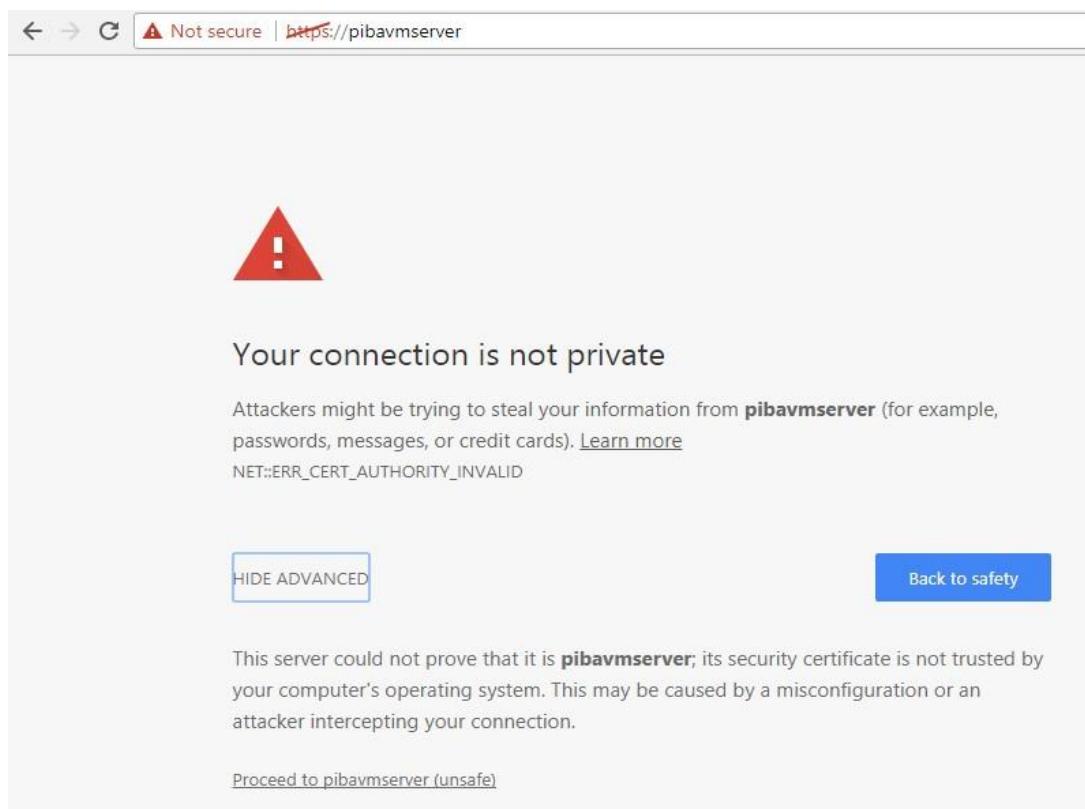
- Disconnect and Click on connect in **ssms** to login with SQL Server authentication to create database with following SQL credentials



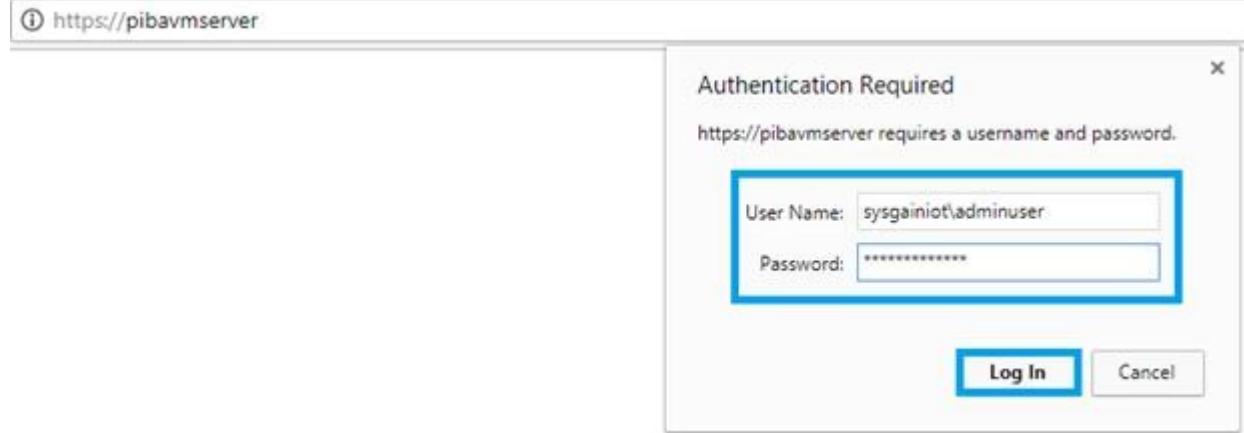
- Go to the **SQLServer Management Studio**, right-click on **Database**, select **New Database**, and give the Database name as **PIBAView**. Click on **Ok**.



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	✚ Modify View Modify existing data view	✖ Remove View Remove selected view
Lock	Name	Run Status	Type

3. Click on **Administration**.

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

≡ PI Integrator for Business Analytics

📁 [My Views](#)
Manage your data views

✍ [Create New Asset View](#)
Build a data view starting with your asset hierarchy

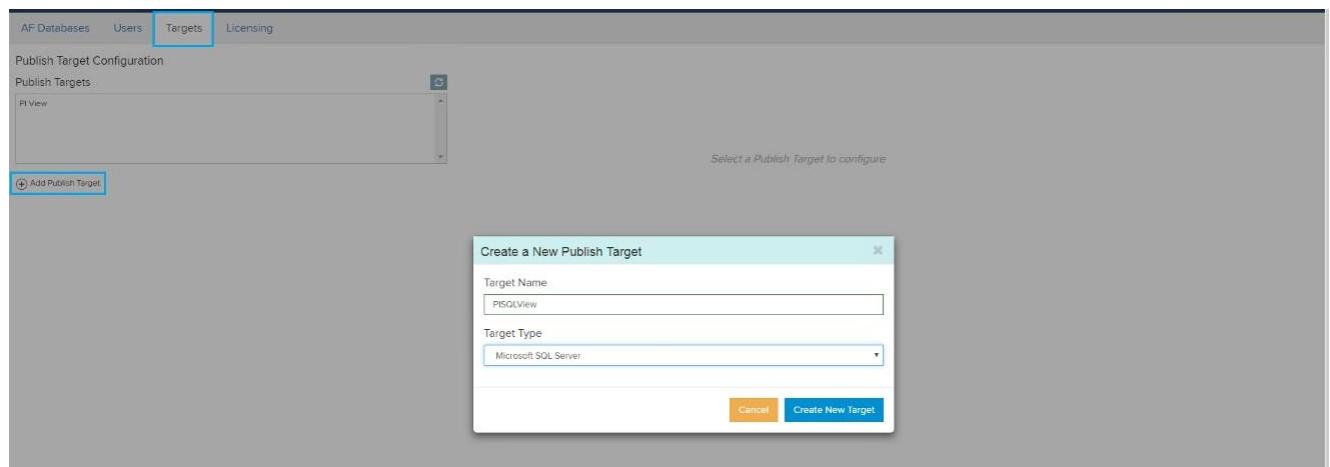
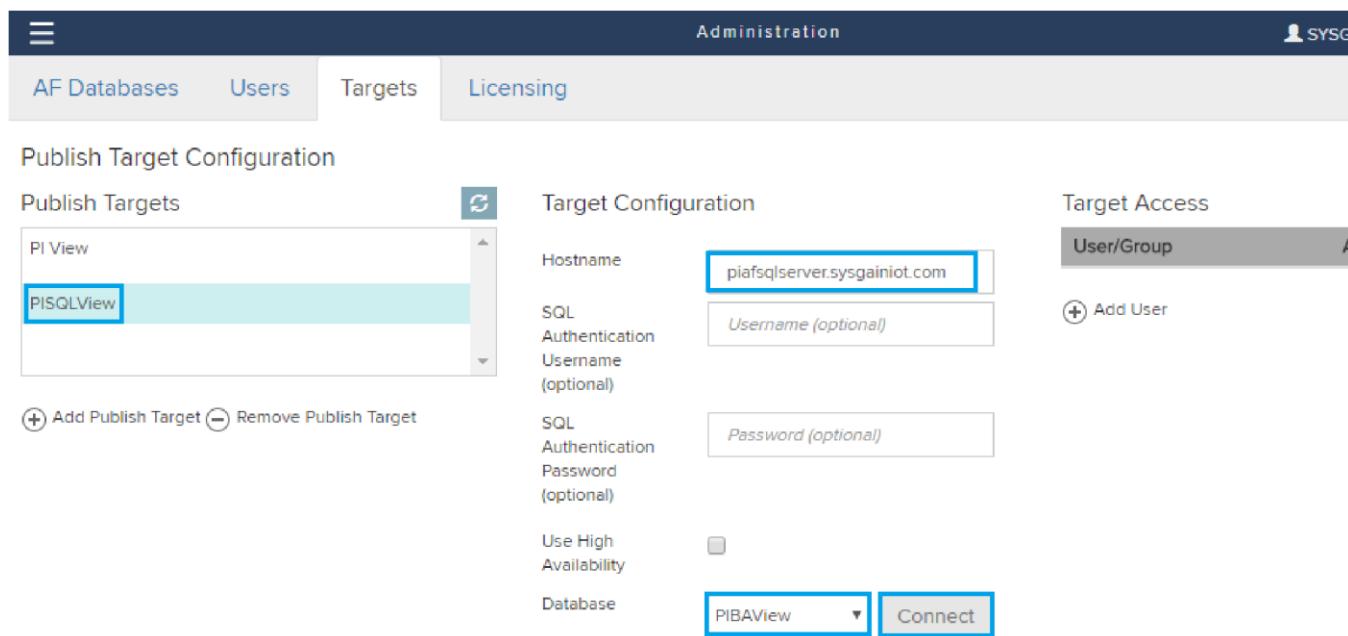
✍ [Create New Event View](#)
Build a data view starting with your event frame hierarchy

🔧 [Administration](#)
Manage servers users and targets

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

Enter Target Name as **PISQLView**.

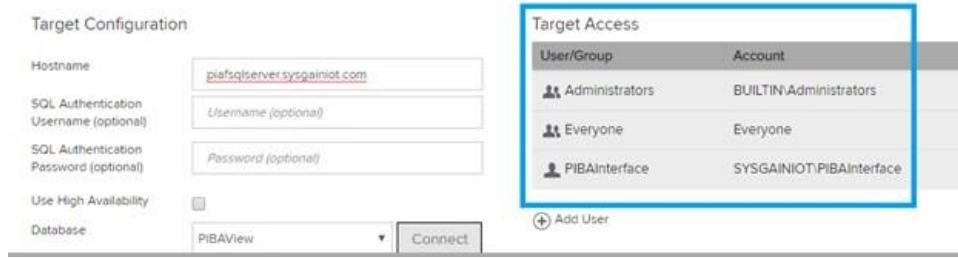
Select Target type as **Microsoft SQL Server** from drop down. After that click on create new target.

Field	Value
Hostname	piafsqlserver.sysgainiot.com
SQL Authentication	Username (optional)
Username (optional)	
SQL Authentication	Password (optional)
Password (optional)	
Use High Availability	<input type="checkbox"/>
Database	PIBAView
Connect	

-
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**

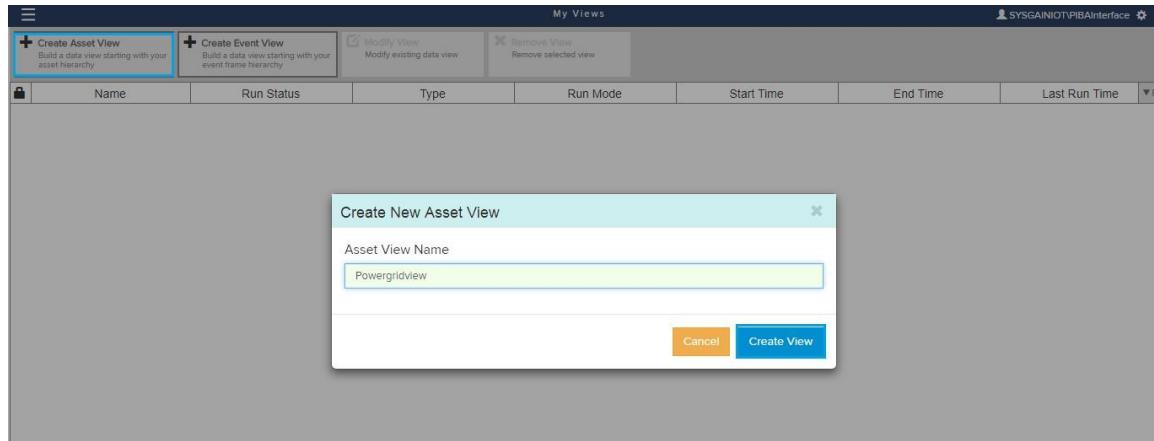
6. You can view the created **target access**



The screenshot shows two windows side-by-side. On the left is the 'Target Configuration' window, which includes fields for Hostname (piawsqiserver.sysgainiot.com), SQL Authentication Username (optional), SQL Authentication Password (optional), and Database (PIBAView). A 'Connect' button is at the bottom right. On the right is the 'Target Access' window, which displays a table of users and their accounts:

User/Group	Account
Administrators	BUILTIN\Administrators
Everyone	Everyone
PIBAInterface	SYSGAINIOT\PIBAInterface

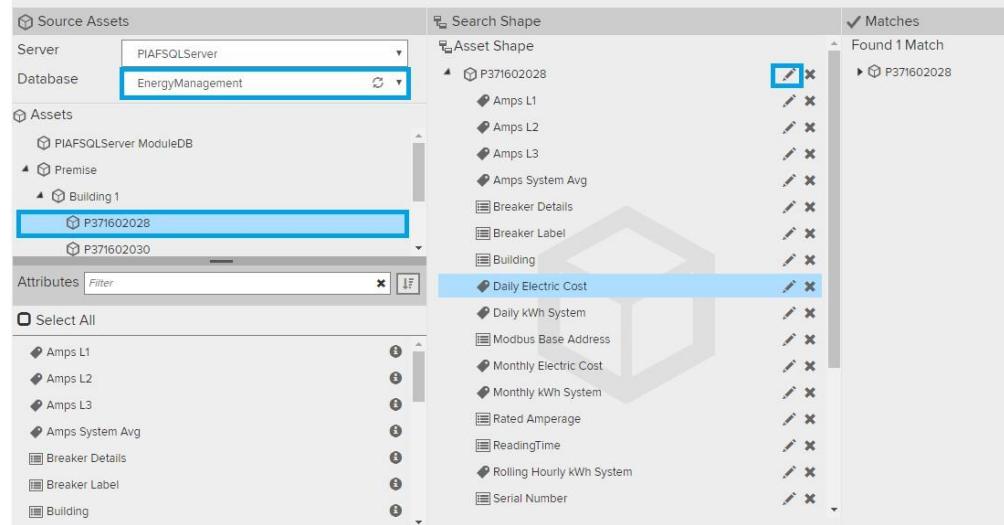
7. Click on **Create Asset view**. Set the Asset View Name as **PowergridView** and click on **Create View**.



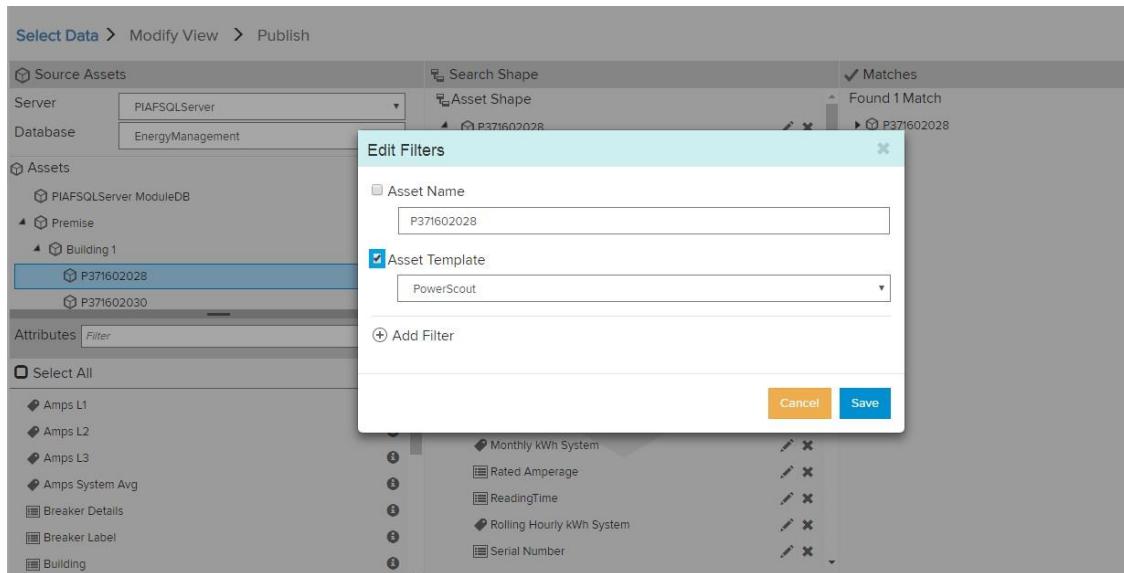
The screenshot shows a 'Create New Asset View' dialog box overlaid on a main interface. The dialog box has 'Asset View Name' set to 'Powergridview' and two buttons at the bottom: 'Cancel' and 'Create View'. In the background, there are tabs for 'Create Asset View', 'Create Event View', 'Modify View', and 'Remove View'. The main interface has columns for Name, Run Status, Type, Run Mode, Start Time, End Time, and Last Run Time.

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**.

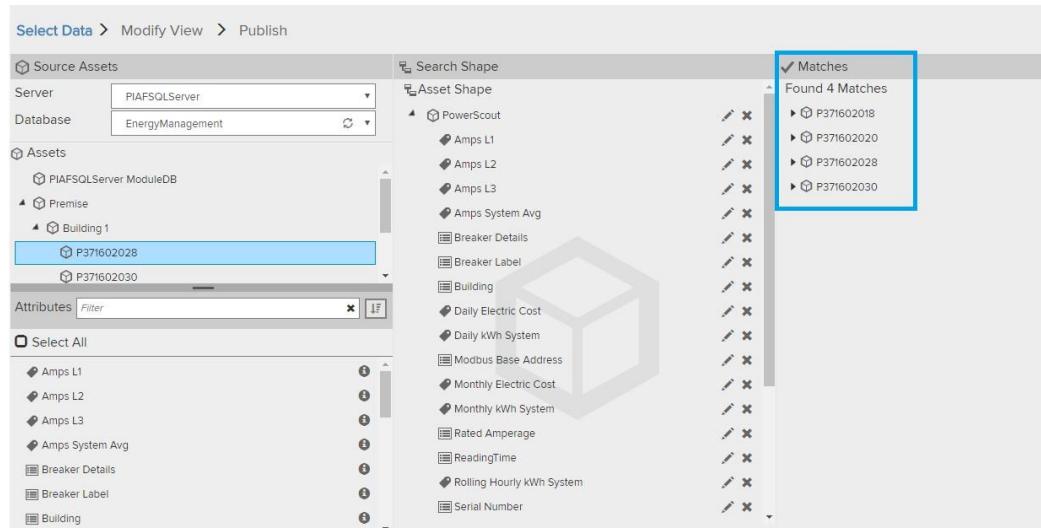
Select Data > Modify View > Publish



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

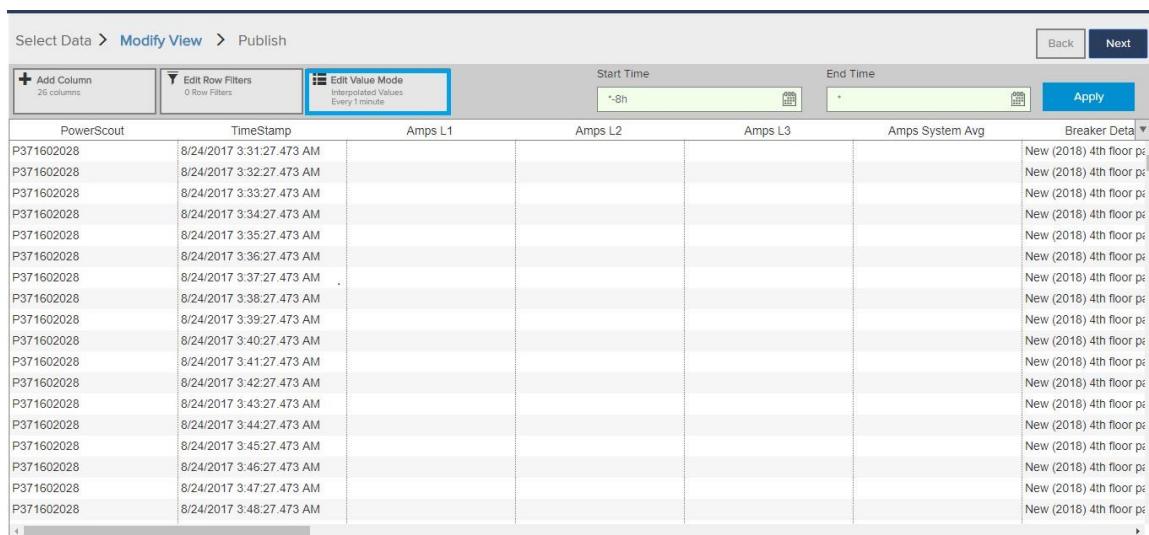


10. You will see the number of matched found on the right-hand side. Then click on **Next**.



The screenshot shows the 'Select Data > Modify View > Publish' interface. In the 'Source Assets' section, 'PIAFSQLServer' is selected as the Server and 'EnergyManagement' as the Database. Under 'Assets', 'PIAFSQLServer ModuleDB' is expanded, showing 'Premise' and 'Building 1'. 'Building 1' contains two items: 'P371602028' and 'P371602030', with 'P371602028' highlighted. In the 'Attributes' section, several options like 'Amps L1', 'Amps L2', etc., are listed. On the right, a 'Search Shape' panel lists various asset types such as 'PowerScout', 'Amps L1', etc. A 'Matches' section at the bottom right shows 'Found 4 Matches' with four entries: 'P371602018', 'P371602020', 'P371602028', and 'P371602030', each preceded by a small icon.

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



The screenshot shows the 'Select Data > Modify View > Publish' interface with the 'Edit Value Mode' button highlighted. The table below has columns for 'PowerScout', 'TimeStamp', 'Amps L1', 'Amps L2', 'Amps L3', 'Amps System Avg', and 'Breaker Details'. The 'TimeStamp' column shows dates from 8/24/2017 to 8/24/2017. The 'Amps L1' column shows values starting from 3:31:27.473 AM. The 'Breaker Details' column shows 'New (2018) 4th floor p'. There are buttons for 'Add Column', 'Edit Row Filters', and 'Edit Value Mode' at the top left. At the top right, there are 'Back', 'Next', and 'Apply' buttons. The 'Start Time' and 'End Time' fields are set to '-8h'.

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

Select Data > Modify View > Publish

PowerScout	TimeStamp	Amps L1	Amps L2	Amps L3	Amps System Avg	Breaker Detail
P371602018	8/24/2017 4:44:07.916 AM	99.541	100.724	100.243	100.243	New (2013) 3rd floor pi
P371602018	8/24/2017 4:45:07.804 AM				60.528	New (2013) 3rd floor pi
P371602018	8/24/2017 4:46:07.679 AM				20.813	New (2013) 3rd floor pi
P371602018	8/24/2017 4:47:07.546 AM				112.100	New (2013) 3rd floor pi
P371602018	8/24/2017 4:48:07.413 AM				93.819	New (2013) 3rd floor pi
P371602018	8/24/2017 4:49:07.263 AM				91.097	New (2013) 3rd floor pi
P371602018	8/24/2017 4:49:42.153 AM				30.298	New (2013) 3rd floor pi
P371602018	8/24/2017 4:50:07.088 AM				109.811	New (2013) 3rd floor pi
P371602018	8/24/2017 4:50:42.042 AM				37.587	New (2013) 3rd floor pi
P371602018	8/24/2017 4:51:06.902 AM				18.956	New (2013) 3rd floor pi
P371602018	8/24/2017 4:51:41.923 AM				128.875	New (2013) 3rd floor pi
P371602018	8/24/2017 4:52:06.769 AM				110.243	New (2013) 3rd floor pi
P371602018	8/24/2017 4:52:41.806 AM	67.251	68.049	67.725	67.725	New (2013) 3rd floor pi
P371602018	8/24/2017 4:53:06.645 AM	70.034	70.866	70.528	70.528	New (2013) 3rd floor pi
P371602018	8/24/2017 4:53:41.689 AM	27.813	28.144	28.009	28.009	New (2013) 3rd floor pi
P371602018	8/24/2017 4:54:06.530 AM	77.272	78.190	77.817	77.817	New (2013) 3rd floor pi
P371602018	8/24/2017 4:54:41.571 AM	35.051	35.468	35.298	35.298	New (2013) 3rd floor pi
P371602018	8/24/2017 4:55:06.414 AM	37.835	38.284	38.102	38.102	New (2013) 3rd floor pi

Edit Value Mode

Sampled Values

- Sample values every minutes
- Use Key Column: Amps L1
- Interpolate
- Exact

Save Changes

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

Select Data > Modify View > Publish

Target Configuration

PISQLView

Run Once

Run on a Schedule

First Run

Start Date: *

Recur every minutes

Summary

Shape and Matches

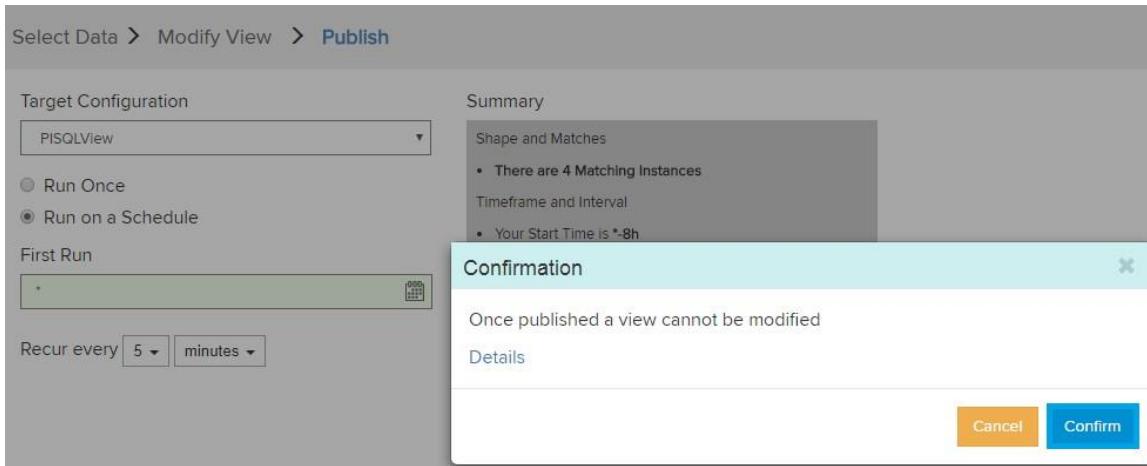
- There are 4 Matching Instances

Timeframe and Interval

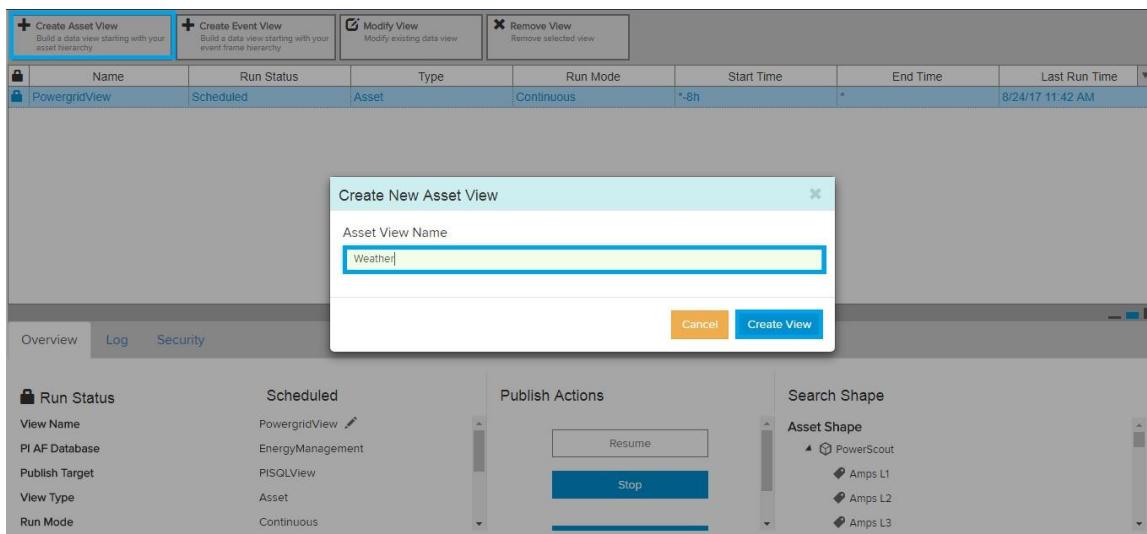
- Your Start Time is *-8h
- Your End Time is *
- Your Time Interval gets an interpolated measurement based on column Amps L1

Publish

14. Click on **Confirm**.



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



Name	Run Status	Type	Run Mode	Start Time	End Time	Last Run Time
PowergridView	Scheduled	Asset	Continuous	*-8h	*	8/24/17 11:42 AM

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

Select Data > Modify View > Publish

Source Assets

- Server: PIAFSQLServer
- Database: EnergyManagement
- Assets:
 - PIAFSQLServer ModuleDB
 - Premise
 - Weather**
 - Wireless Tags

Attributes Filter

Deselect All

- 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

Found 1 Match

- Weather

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

Select Data > Modify View > Publish

Source Assets

- Server: PIAFSQLServer
- Database: EnergyManagement
- Assets:
 - PIAFSQLServer ModuleDB
 - Premise
 - Weather**
 - Wireless Tags

Attributes Filter

Deselect All

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

Edit Filters

Asset Name
Weather

Asset Template
PowerScout

Add Filter

Cancel **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

- PIAFSQLServer ModuleDB
- Premise
 - Weather
 - Wireless Tags

Attributes: Filter

Deselect All

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

Search Shape

Asset Shape

Weather

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

Matches

Found 1 Match

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

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

Select Data > Modify View > Publish

Back
Next

Add Column		Edit Row Filters		Edit Value Mode		Start Time	End Time	Apply	
9 columns		0 Row Filters		Interpolated Values Key on Pressure		-1h	+1h	Cancel	Save Changes
Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather	Wind Direction	Wind Speed
Weather	8/24/2017 4:48:07 AM	29.207	50.714	51.801	3.017	Overcast	North	7.241	
Weather	8/24/2017 4:49:07.3...	31.213				Variable	Variable	19.281	
Weather	8/24/2017 4:49:42.2...	31.922				Sun Light...	Northwest	23.531	
Weather	8/24/2017 4:50:07.1...	29.220				Fog/Mist	North	7.320	
Weather	8/24/2017 4:50:42.1...	30.709				Cloudy	Southeast	16.255	
Weather	8/24/2017 4:51:06.9...	29.011				Cloudy	North	6.064	
Weather	8/24/2017 4:51:41.9...	30.932				Cloudy	Southeast	17.590	
Weather	8/24/2017 4:52:06.8...	28.928				Cloudy	West	5.566	
Weather	8/24/2017 4:52:41.8...	29.719				Cloudy	South	10.314	
Weather	8/24/2017 4:53:06.7...	31.715				Cloudy	Northwest	22.290	
Weather	8/24/2017 4:53:41.7...	28.506				Cloudy	West	3.038	
Weather	8/24/2017 4:54:06.5...	31.938				Thunderstorm Light...	Northwest	23.625	
Weather	8/24/2017 4:54:41.6...	30.639	56.450	52.076	3.644	Thunderstorm Light...	Northwest		
Weather	8/24/2017 4:55:06.4...	28.160	65.982	72.929	6.598	Light Rain Fog/Mist	Southeast	15.836	
Weather	8/24/2017 4:55:41.5...	30.862	4.002	36.361	0.400	Light Rain	East	0.960	
Weather	8/24/2017 4:56:06.3...	30.947	71.546	76.212	7.155	A Few Clouds	Southeast	17.171	
Weather	8/24/2017 4:56:41.3...	28.214	73.686	77.474	7.369	A Few Clouds	Southeast	17.685	
Weather	8/24/2017 4:57:06.2...	29.735	5.349	37.156	0.535	unknown Precip	East	1.284	
Weather	8/24/2017 4:57:41.2...	28.437	43.369	59.588	4.337	Fair and Breezy	South	10.409	
Weather			10.913	40.439	1.091	A Few Clouds	East	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		End Time			
						~-1h					
										Apply	
Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather	Wind Direction	Wind Speed		
Weather	8/24/2017 4:48:07.4...	29.207	30.171	51.801	3.017	Overcast	North	7.241			
Weather	8/24/2017 4:49:07.3...	31.213	80.336	81.399	8.034	Heavy Rain	Variable	19.281			
Weather	8/24/2017 4:49:42.2...	31.922	98.045	91.847	9.805	Thunderstorm Light ...	Northwest	23.531			
Weather	8/24/2017 4:50:07.1...	29.220	30.502	51.996	3.050	Fog/Mist	North	7.320			
Weather	8/24/2017 4:50:42.1...	30.709	67.729	73.960	6.773	Light Rain Fog/Mist	Southeast	16.255			
Weather	8/24/2017 4:51:06.9...	29.011	25.268	48.908	2.527	Partly Cloudy	North	6.064			
Weather	8/24/2017 4:51:41.9...	30.932	73.293	77.243	7.329	A Few Clouds	Southeast	17.590			
Weather	8/24/2017 4:52:06.8...	28.928	23.190	47.682	2.319	Partly Cloudy	West	5.566			
Weather	8/24/2017 4:52:41.8...	29.719	42.977	59.356	4.298	Fair and Breezy	South	10.314			
Weather	8/24/2017 4:53:06.7...	31.715	92.874	88.796	9.287	Thunderstorm in 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	17.665			
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

Run Once

Run on a Schedule

First Run

*

Recur every minutes

Summary

Shape and Matches

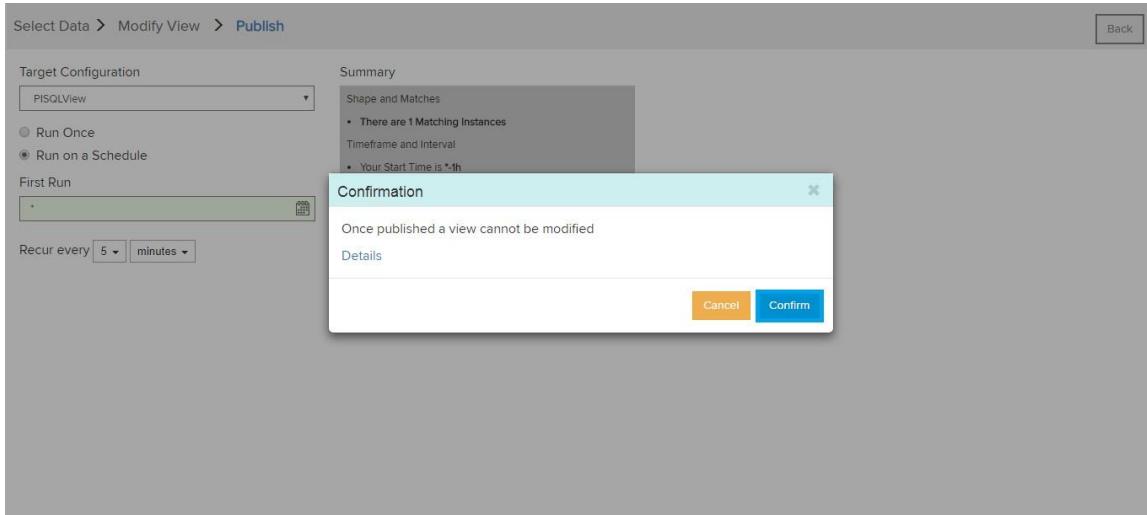
- There are 1 Matching Instances

Timeframe and Interval

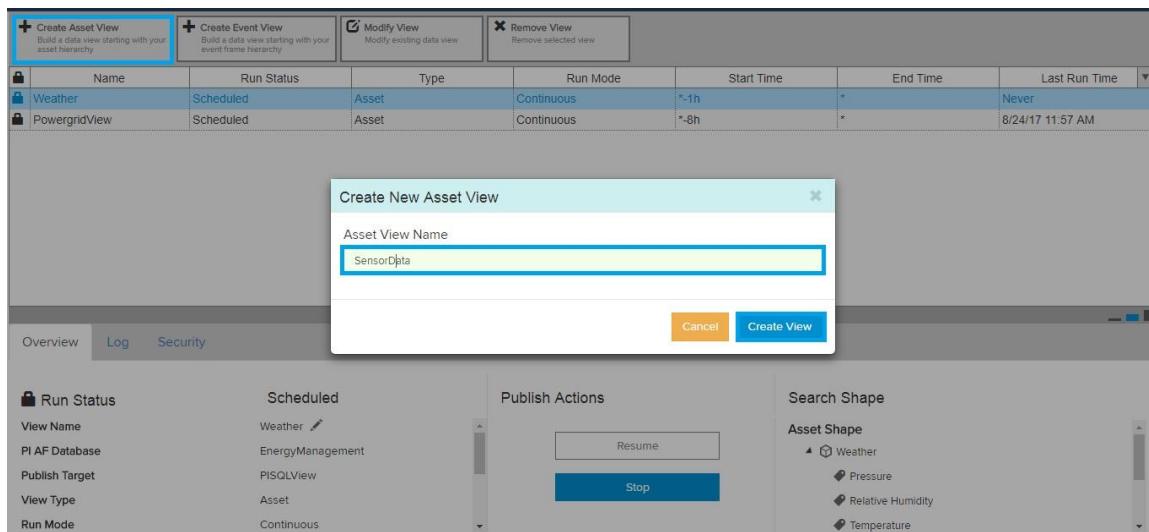
- Your Start Time is *-1h
- Your End Time is *
- Your Time Interval gets an interpolated measurement based on column Pressure

Publish

22. Click on **Confirm**.



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



Name	Run Status	Type	Run Mode	Start Time	End Time	Last Run Time
Weather	Scheduled	Asset	Continuous	*-1h	*	Never
PowergridView	Scheduled	Asset	Continuous	*-8h	*	8/24/17 11:57 AM

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

Select All

- 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

Select All

- Brightness
- Humidity
- Name
- Temperature

Search Shape

Asset Shape

Wireless Tag Template

- Brightness
- Humidity
- Name
- Temperature

Matches

Found 2 Matches

- Light Sensor 1
- Office 1

- Brightness
- Humidity
- Name
- Temperature

Next

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

Select Data > Modify View > Publish

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	

Start Time: -8h End Time:

Edit Value Mode

Sampled Values

Sample values every minutes

Use Key Column

Interpolate Exact

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

Select Data > Modify View > Publish

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

Start Time: End Time:

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

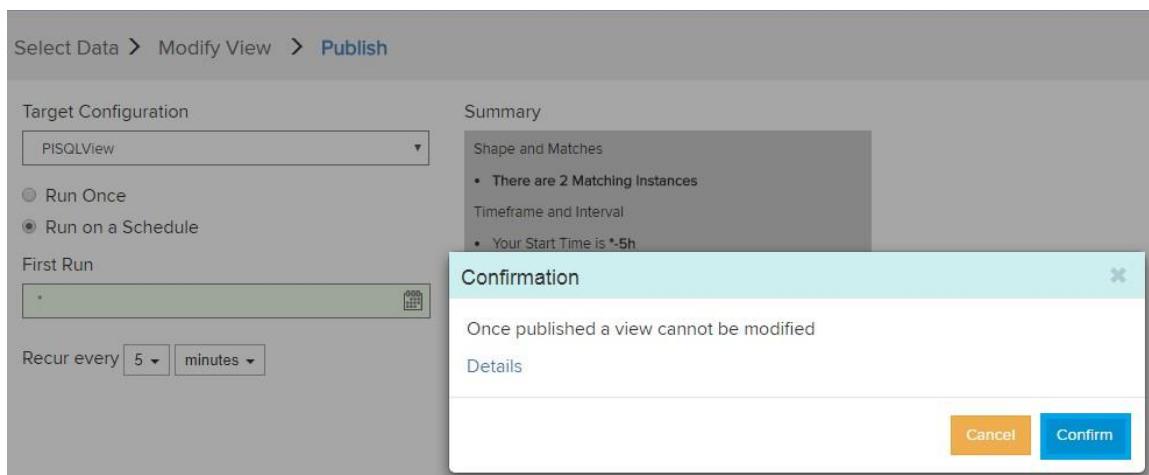
Timeframe and Interval

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

Recur every minutes

Publish

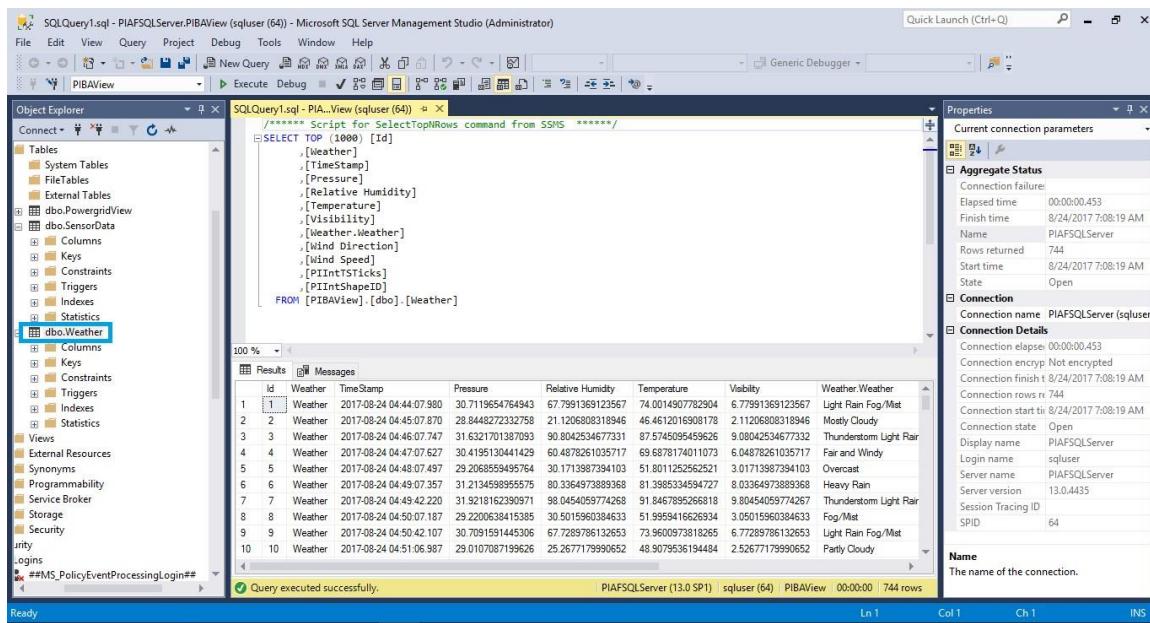
29. Click on **Confirm**.



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**.



The screenshot shows the SSMS interface with the following details:

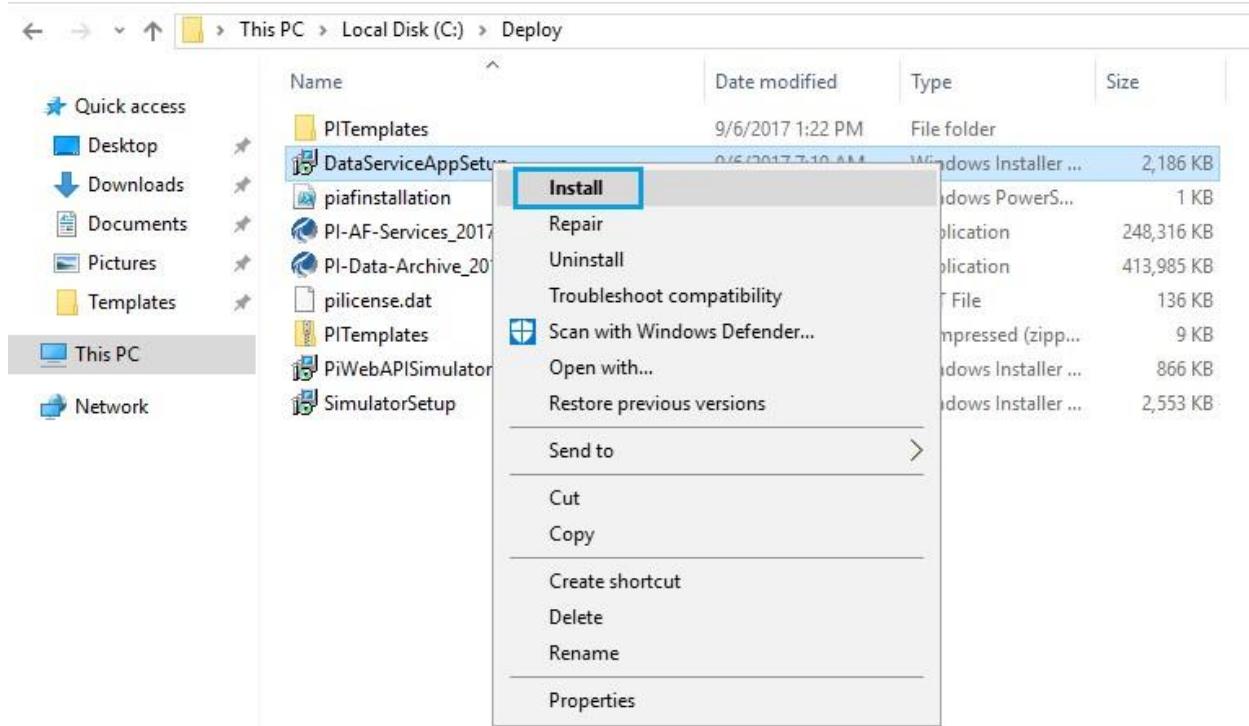
- Object Explorer:** Shows the database structure including Tables, Views, and other objects.
- Query Editor:** Displays a T-SQL script:

```
===== Script for SelectTopNRows command from SSMS =====
SELECT TOP (1000) [Id]
    ,[Weather]
    ,[TimeStamp]
    ,[Pressure]
    ,[Relative Humidity]
    ,[Temperature]
    ,[Visibility]
    ,[Weather.Weather]
    ,[Wind Direction]
    ,[Wind Speed]
    ,[PIintSticks]
    ,[PIintShapeID]
FROM [PIBAView].[dbo].[Weather]
```
- Results Grid:** Shows 10 rows of data from the Weather table:

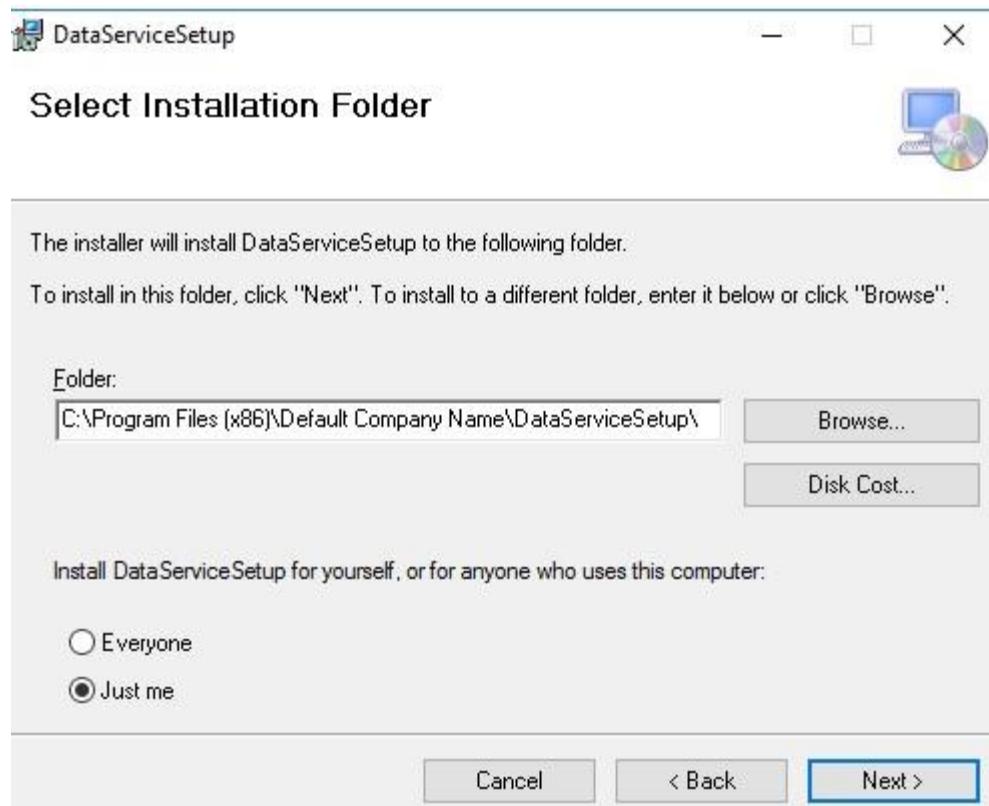
	Id	Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather
1	1	Weather	2017-09-24 04:44:07.980	30.7119654764943	67.7991369123567	74.0014907782904	6.77991369123567	Light Rain	Fog/Mist
2	2	Weather	2017-09-24 04:45:07.870	28.844827232758	21.120680318946	46.46120680318946	2.1120680318946	Misty	Cloudy
3	3	Weather	2017-09-24 04:46:07.747	31.6321701397093	50.8042534677331	87.5745095459626	9.08042534677332	Thunderstorm	Light Rain
4	4	Weather	2017-09-24 04:47:06.727	30.4195130411429	60.4878261035717	69.6878174011073	6.04878261035717	Fair	and Windy
5	5	Weather	2017-09-24 04:48:07.497	29.2068559459764	30.1713987394103	51.801125262521	3.01713987394103	Overscast	
6	6	Weather	2017-09-24 04:49:07.357	31.213458955575	80.3364973889368	81.3985345947277	8.03364973889368	Heavy	Rain
7	7	Weather	2017-09-24 04:49:42.220	31.9218162309071	98.0454059774268	91.8467895268618	9.80454059774267	Thunderstorm	Light Rain
8	8	Weather	2017-09-24 04:50:07.187	29.2200638415385	30.5015960384633	51.9959416626934	3.05015960384633	Fog/Mist	
9	9	Weather	2017-09-24 04:50:42.107	30.7091591445306	67.7289786132653	73.9600973818265	6.77289786132653	Light Rain	Fog/Mist
10	10	Weather	2017-09-24 04:51:06.987	29.0107087199625	25.267717999052	48.9079536194484	2.5267717999052	Party	Cloudy
- Properties Pane:** Shows connection parameters, aggregate status, and detailed connection information including connection name, elapsed time, and session details.

10.2. Install And Run The DataServiceAppSetup

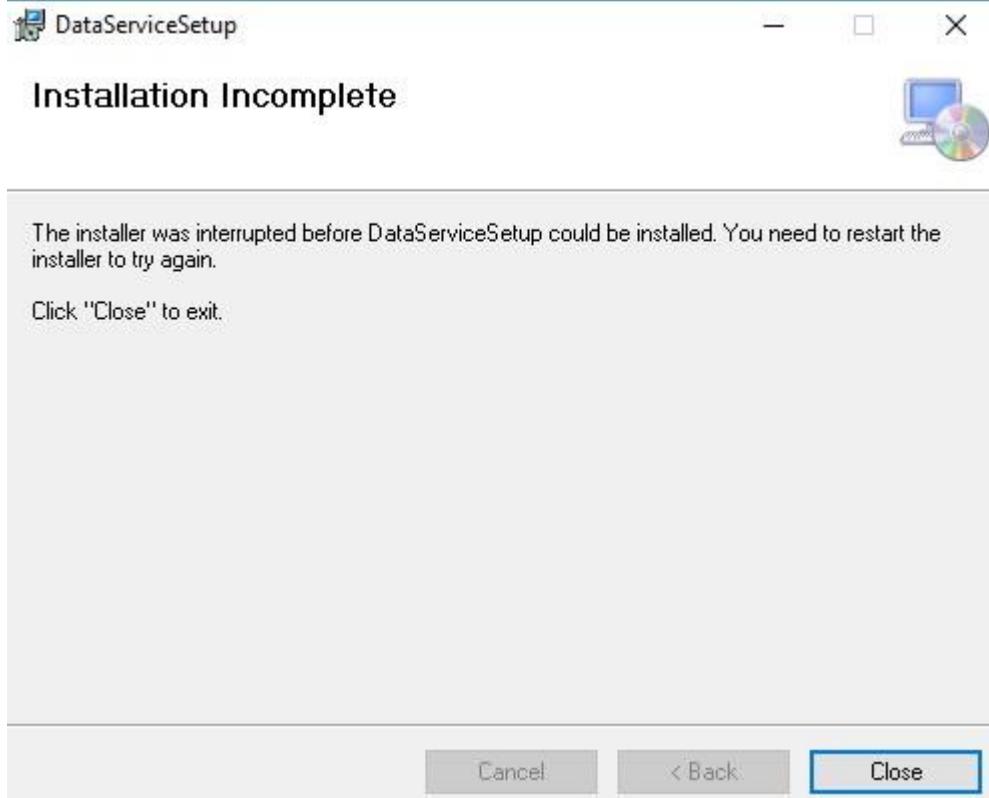
1. Navigate to the **Local Disk (C:) > Deploy > DataServiceAppSetup** and right-click to **Install**.



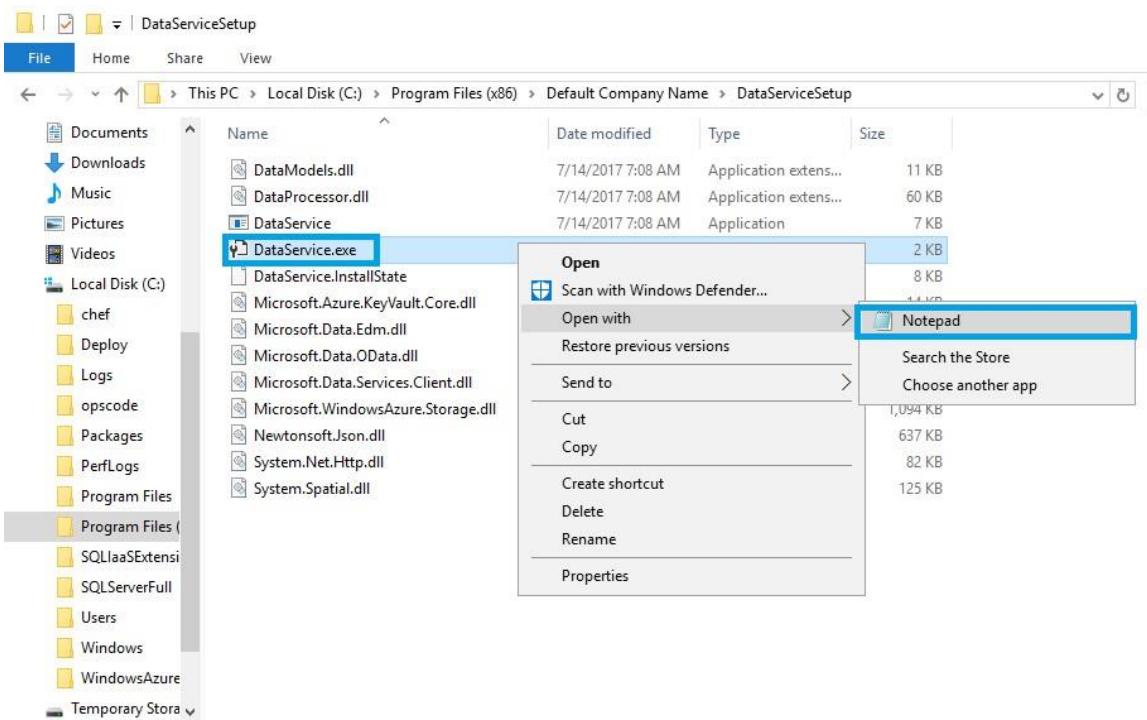
2. Click on **Next**



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

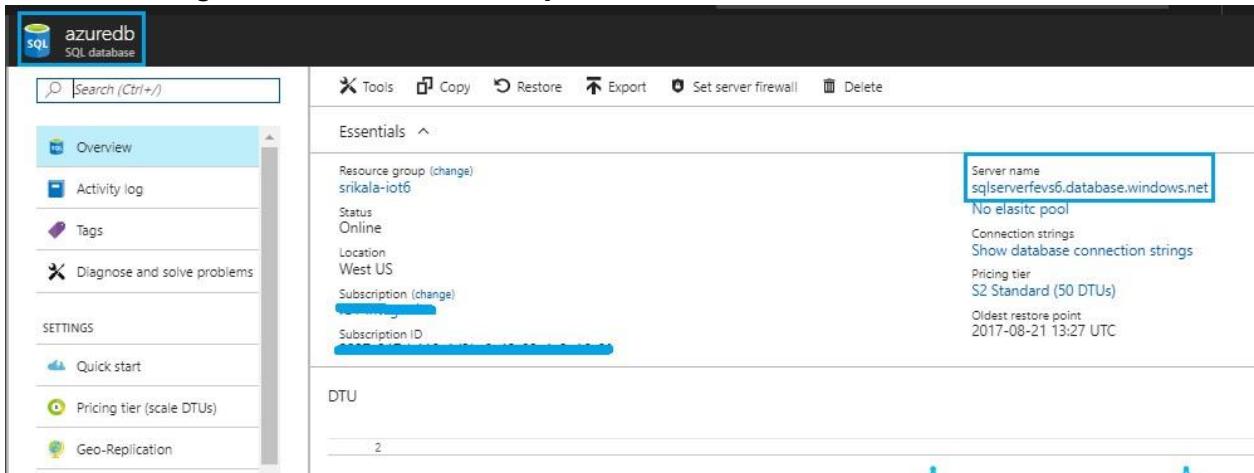


4. Navigate to **Local Disk (C:) > Program Files (*86) > Default company name > Data Services Setup** > Right click on **Dataservice.exe**, then file open with notepad.



- 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)	Deployments
PIAF Integration	12 Succeeded
Subscription ID	[REDACTED]

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: webjobstr4c7xh

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:

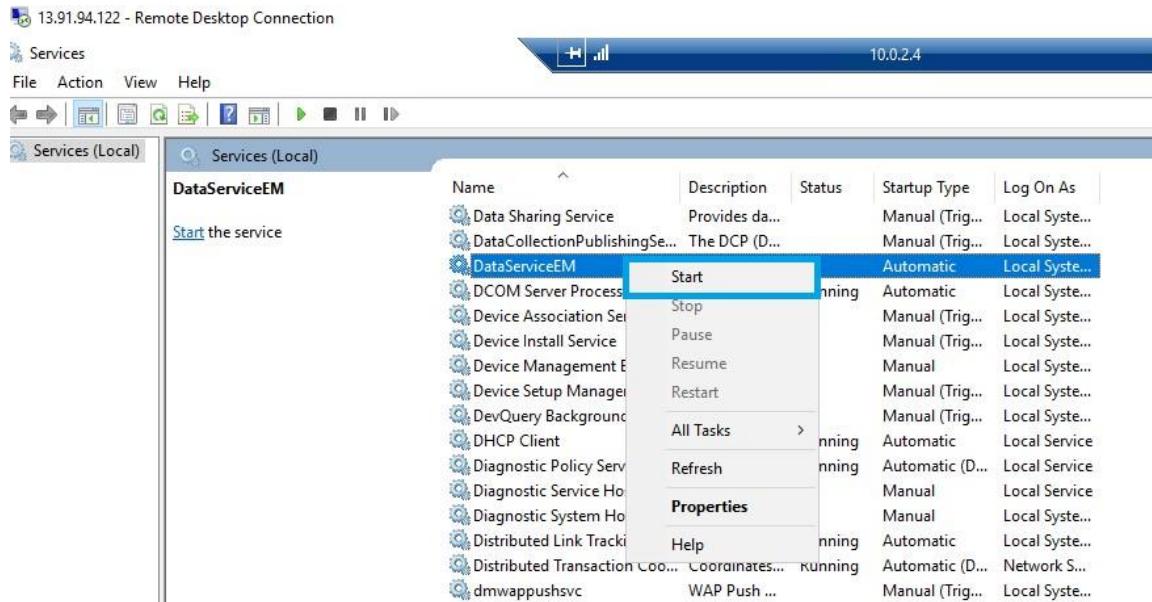
NAME	KEY	CONNECTION STRING
key1	[REDACTED]	DefaultEndpointsProtocol=https;AccountName=web... [REDACTED]
key2	[REDACTED]	DefaultEndpointsProtocol=https;AccountName=web... [REDACTED]

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.

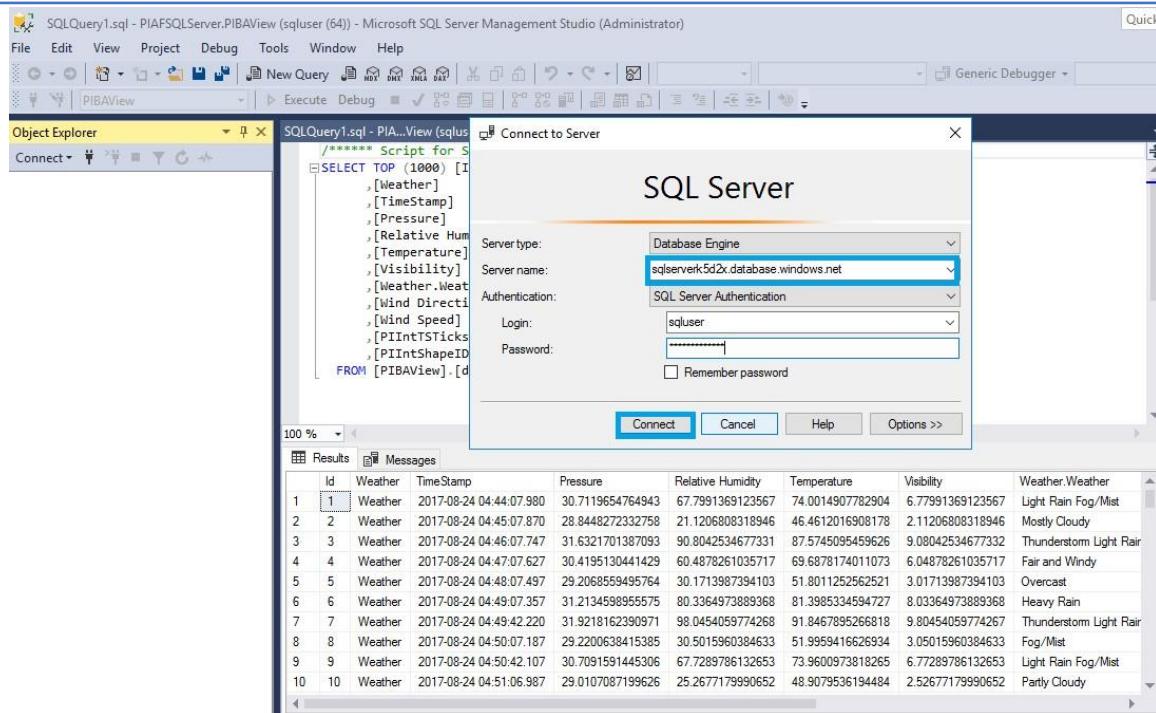
```

<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=sqouser;Password=1234;" />
        <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=webjobstr4c7xh;AccountKey=92PqGkGah0fUko80XXfbmMfrw/ISgJfFgJfQ8dnTSck2;" />
        <add key="PIAServerConnectionString" value="data source=PIAFSQLServer;Initial catalog=PIAView;persist security info=True;user id=sqouser;password=1234;" />
    </appSettings>
    <runtime>
        <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
            <dependentAssembly>
                <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6a6eed" culture="neutral" />
                <bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
            </dependentAssembly>
        </assemblyBinding>
    </runtime>
</configuration>
```

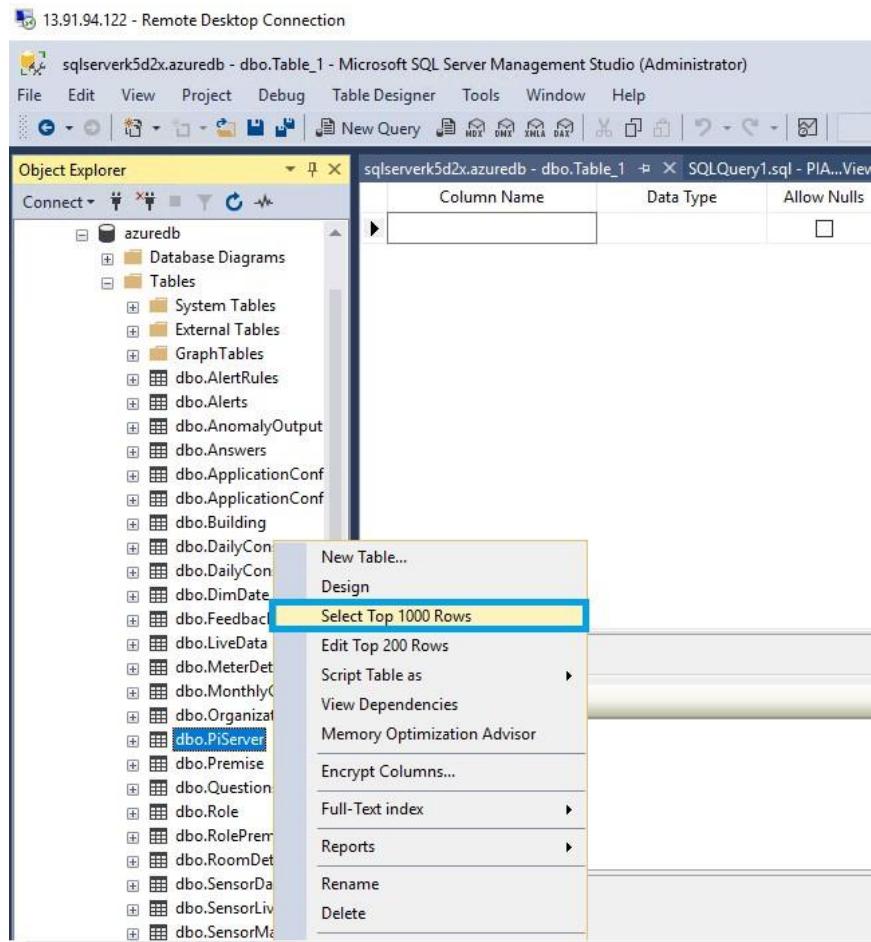
- After updating the values in the data service.exe files, navigate **Start > Service** to start the **DataServicesEM**.



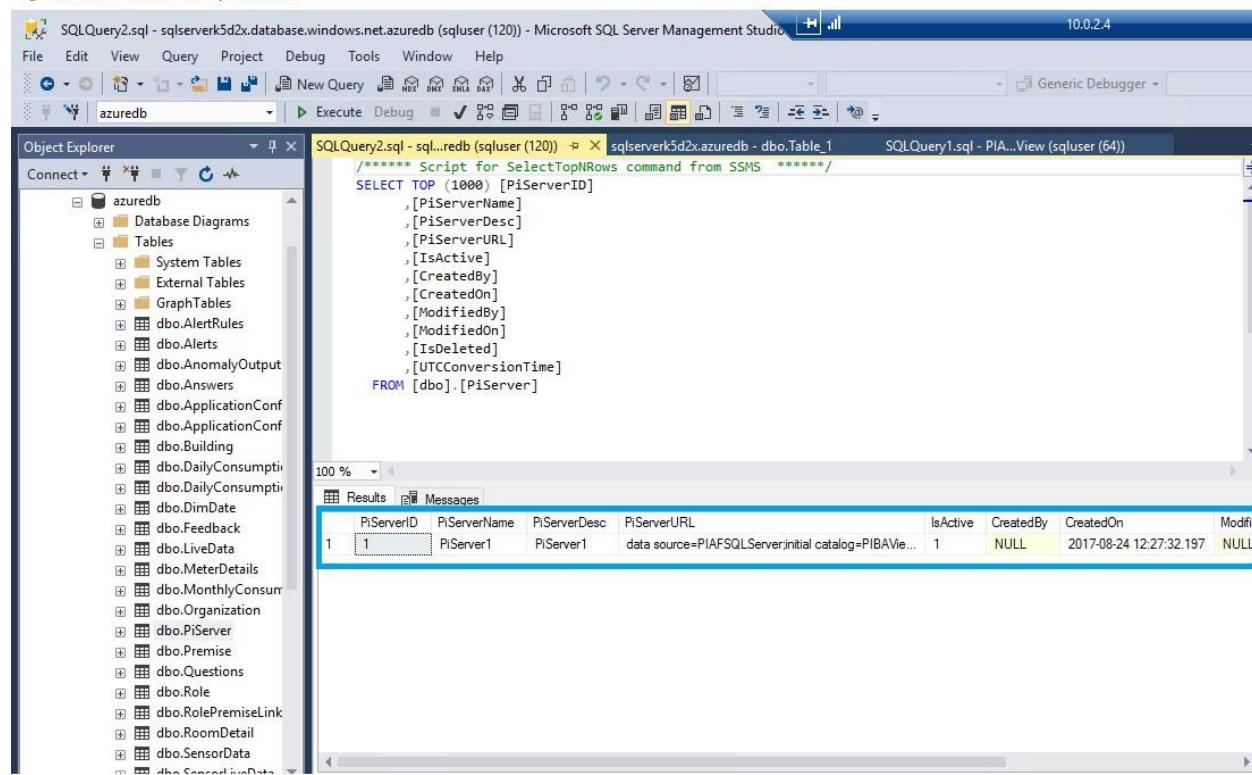
- To check the data, we need to login to SQL server management studio in AF server with azure SQL server name with SQL login credentials and click on **connect**.



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



9. Check the updated table.

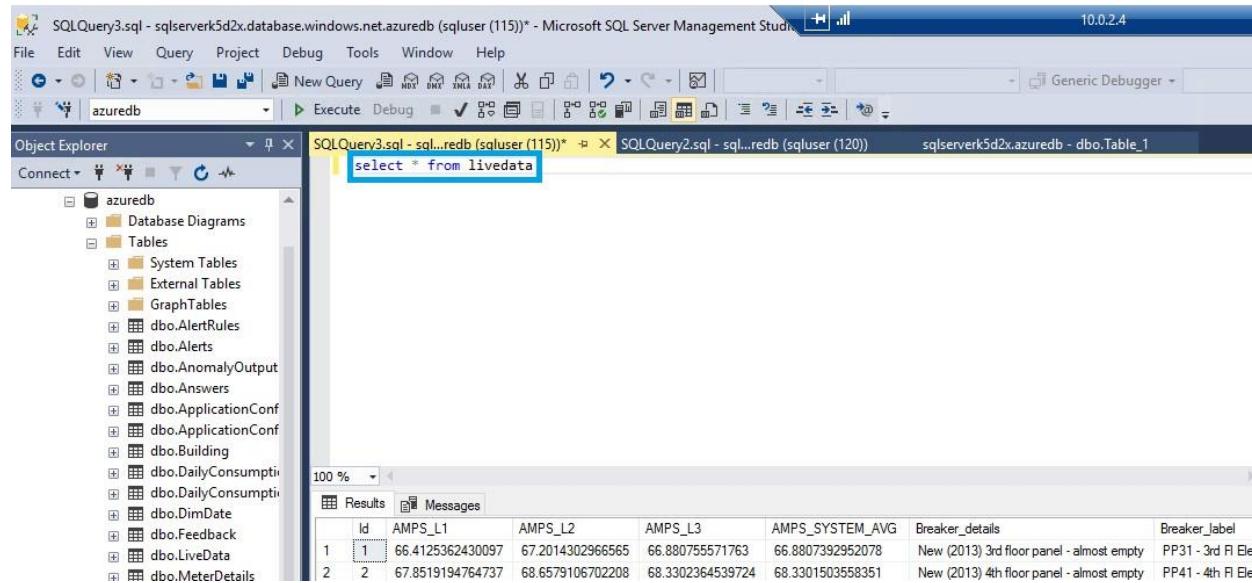


Object Explorer

```
SELECT TOP (1000) [PiServerID]
,[PiServerName]
,[PiServerDesc]
,[PiServerURL]
,[IsActive]
,[CreatedBy]
,[CreatedOn]
,[ModifiedBy]
,[ModifiedOn]
,[IsDeleted]
,[UTCConversionTime]
FROM [dbo].[PiServer]
```

Results

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



Object Explorer

```
select * from livedata
```

Results

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 Ele
2	67.8519194764737	68.6579106702208	68.3302364539724	68.3301503558351	New (2013) 4th floor panel - almost empty	PP41 - 4th Fl Ele

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

File Edit View Query Project Debug Tools Window Help

azuredb

Object Explorer

Connect ▾

- azuredb
 - Database Diagrams
 - Tables
 - System Tables
 - External Tables
 - GraphTables
 - dbo.AlertRules
 - dbo.Alerts
 - dbo.AnomalyOutput
 - dbo.Answers
 - dbo.ApplicationConf
 - dbo.ApplicationConf
 - dbo.Building
 - dbo.DailyConsumpti
 - dbo.DailyConsumpti
 - dbo.DimDate
 - dbo.Feedback
 - dbo.LiveData
 - dbo.MeterDetails
 - dbo.MonthlyConsum
 - dbo.Organization
 - dbo.PiServer

SQLQuery3.sql - sal...redb (sauser (115))*

SQLQuery2.sql

```
select * from building
```

Results Messages

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

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

File Edit View Query Project Debug Tools Window Help

azuredb

Object Explorer

Connect ▾

- azuredb
 - Database Diagrams
 - Tables
 - System Tables
 - External Tables
 - GraphTables
 - dbo.AlertRules
 - dbo.Alerts
 - dbo.AnomalyOutput
 - dbo.Answers
 - dbo.ApplicationConf
 - dbo.ApplicationConf
 - dbo.Building
 - dbo.DailyConsumpti
 - dbo.DailyConsumpti
 - dbo.DimDate
 - dbo.Feedback
 - dbo.LiveData
 - dbo.MeterDetails
 - dbo.MonthlyConsum
 - dbo.Organization
 - dbo.PiServer

SQLQuery3.sql - sal...redb (sauser (115))*

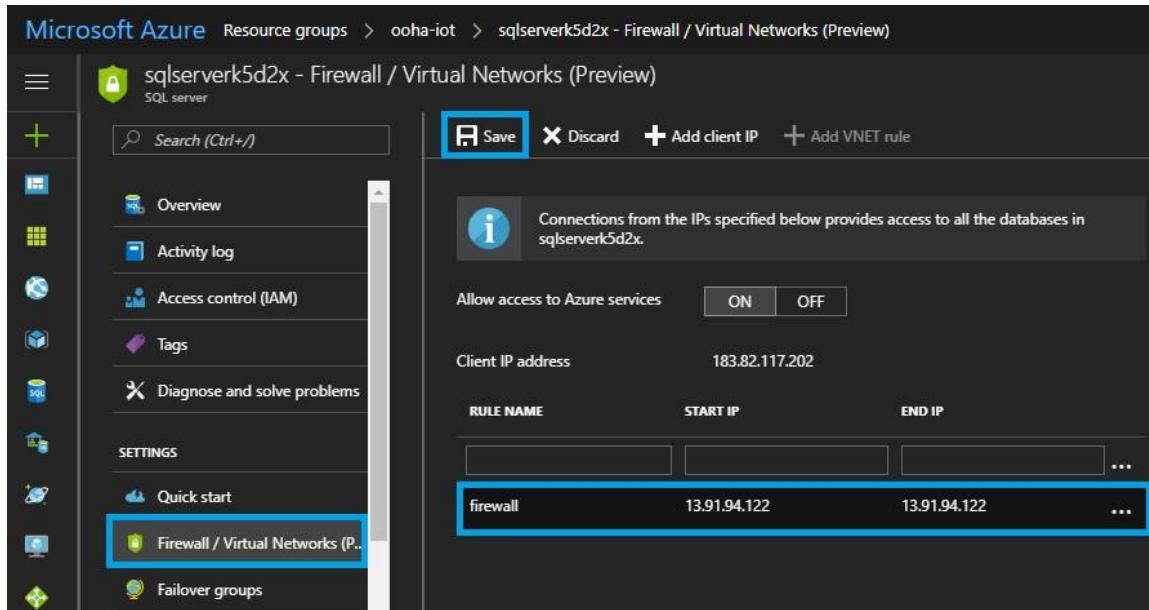
SQLQuery2.sql - sql...redb (sauser (115))*

```
select * from sensormaster
```

Results Messages

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

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



sqlserverk5d2x - Firewall / Virtual Networks (Preview)

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

Allow access to Azure services: **ON**

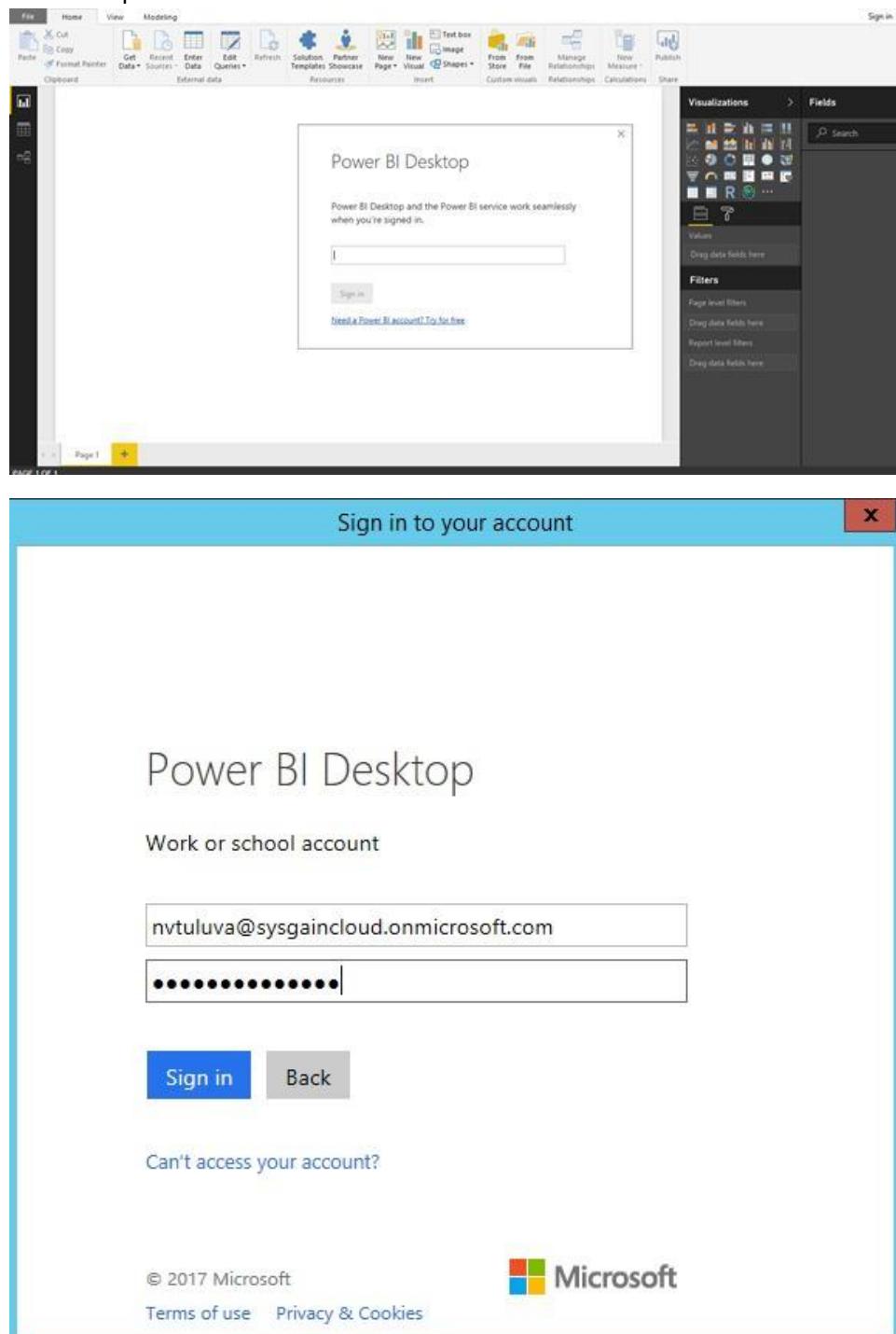
Client IP address: 183.82.117.202

RULE NAME	START IP	END IP
firewall	13.91.94.122	13.91.94.122

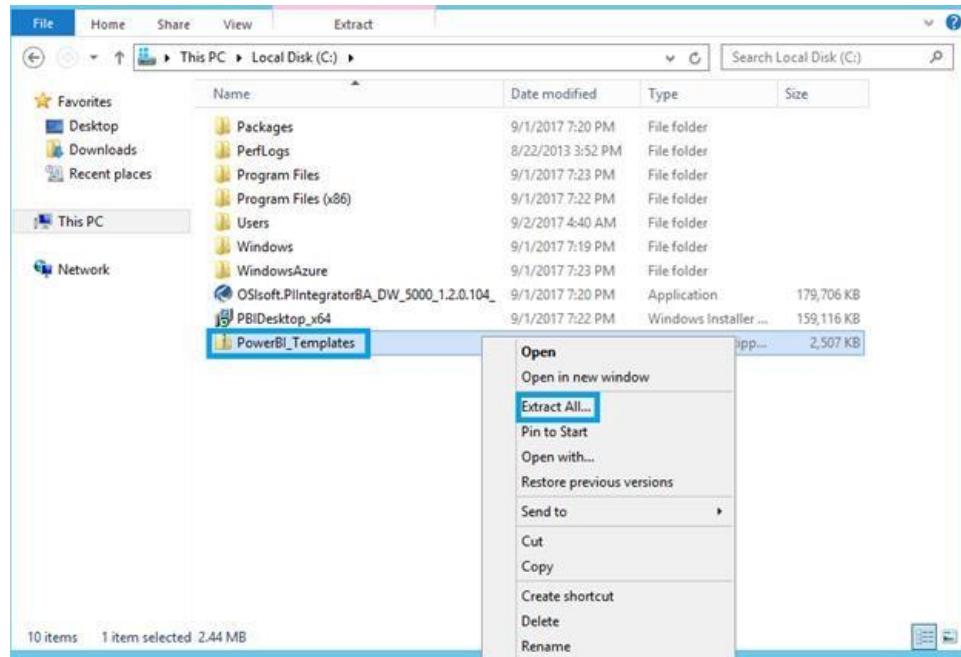
11. Login to the Bastionserver you can see the power BI desktop in Bastionserver desktop. Click on that Power BI desktop.



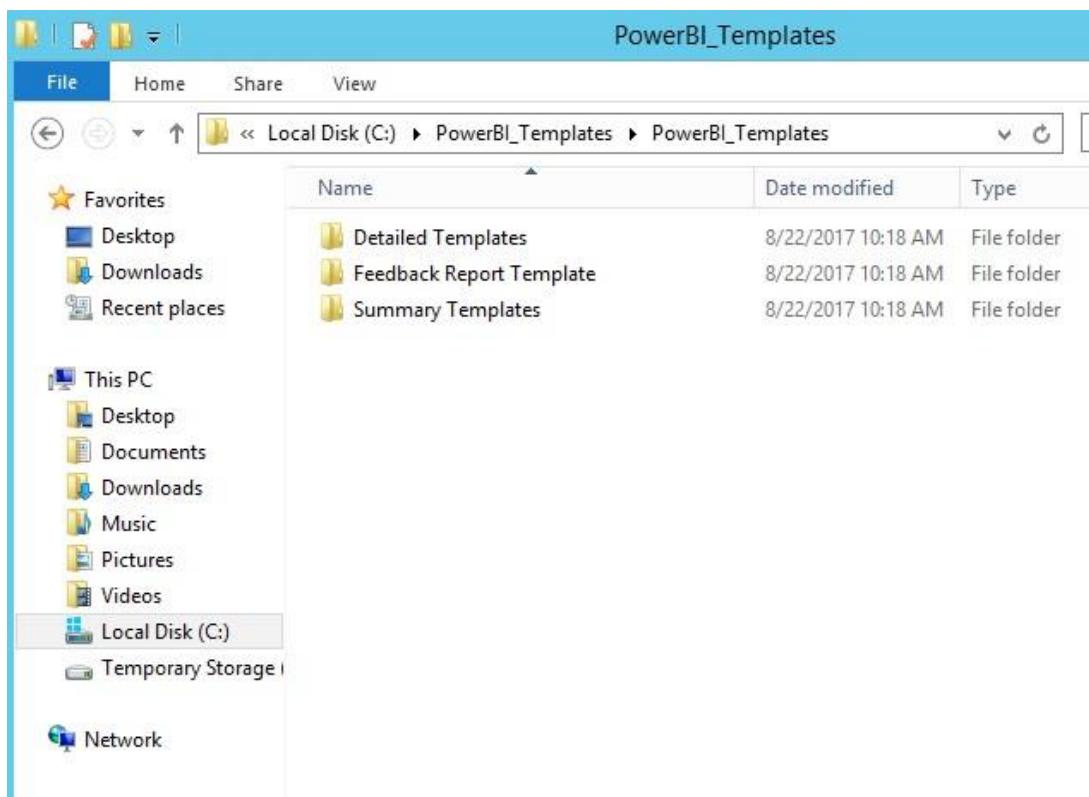
12. Log in with the same credentials used while registration of webapp with power BI you don't need to create a power BI account.



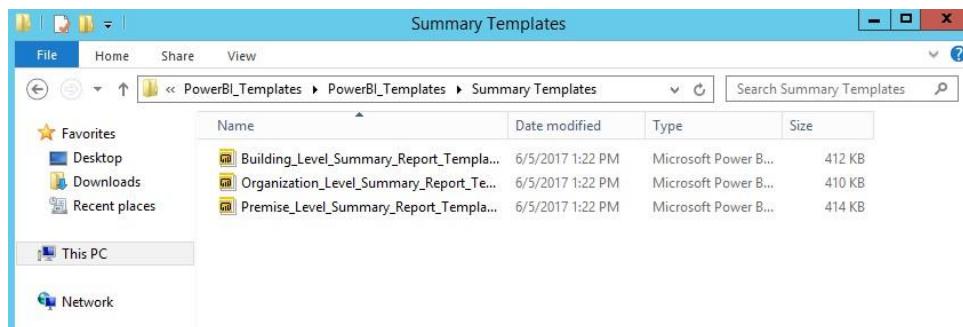
13. In Bastion server, navigate to **Local disk (C:) > unzip the Power Bi templates > Power Bi templates.**



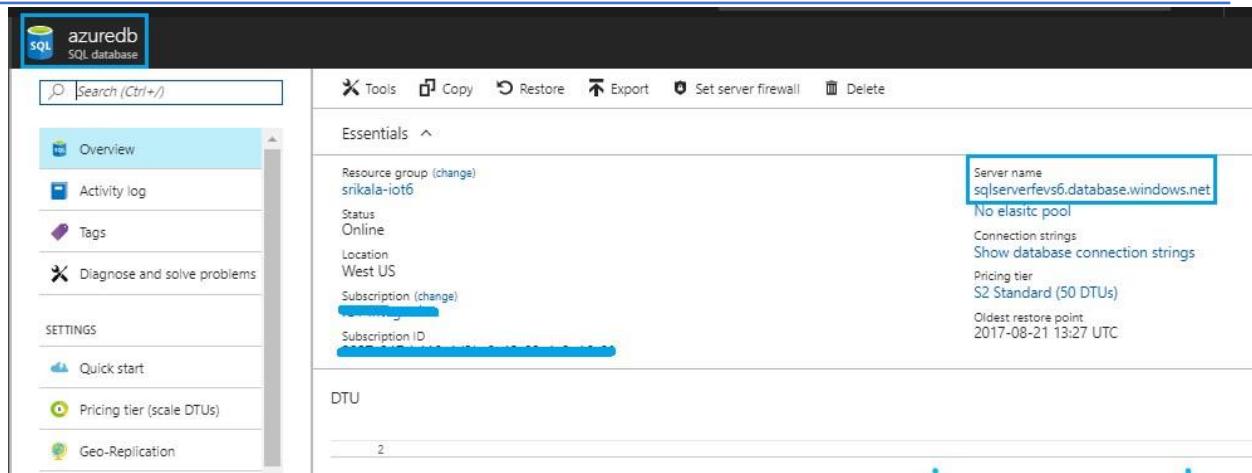
14. You can view Power BI templates in the Local disk (C:)



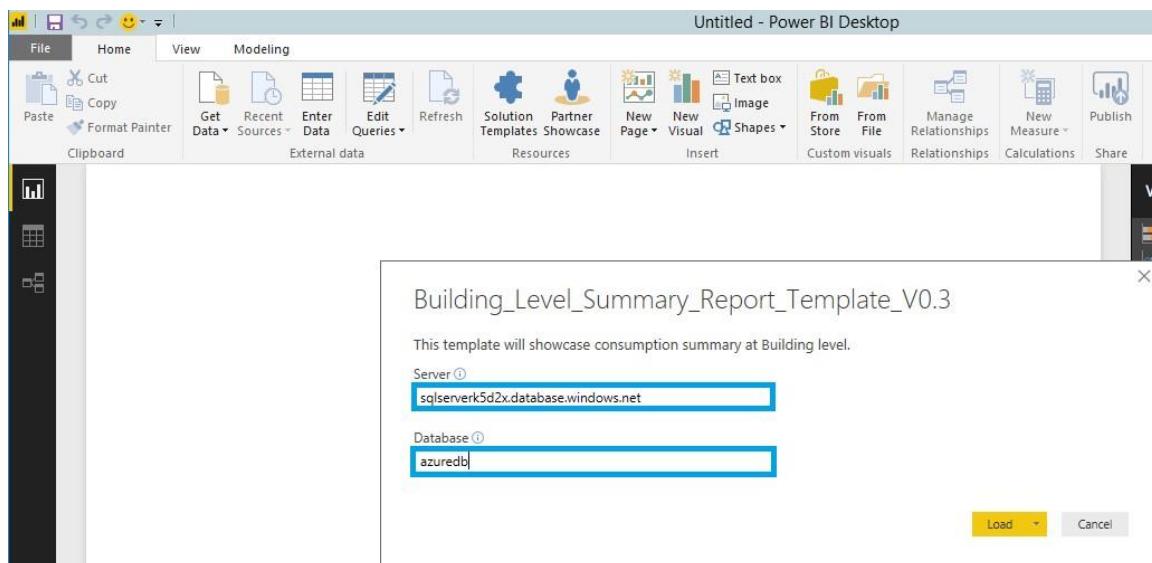
15. Navigate to the summary templates folder, click on "**Building_level_summary templates**" click on keep using Microsoft Power BI Desktop



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**.

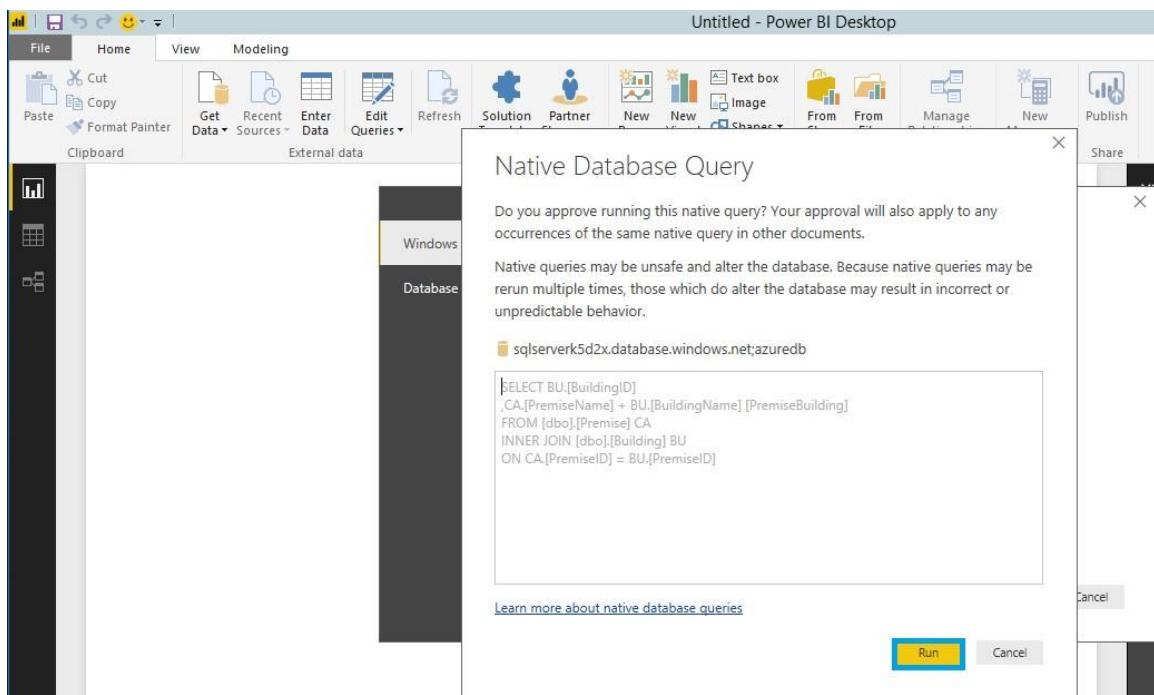


The screenshot shows the Azure portal interface for a SQL database named 'azuredb'. The left sidebar contains navigation links like Overview, Activity log, Tags, Diagnose and solve problems, SETTINGS, Quick start, Pricing tier (scale DTUs), and Geo-Replication. The main content area is titled 'Essentials' and displays resource group (srikala-iot6), status (Online), location (West US), subscription (S2 Standard (50 DTUs)), and connection details (Server name: sqlserverfevs6.database.windows.net). A 'DTU' section shows a value of 2.

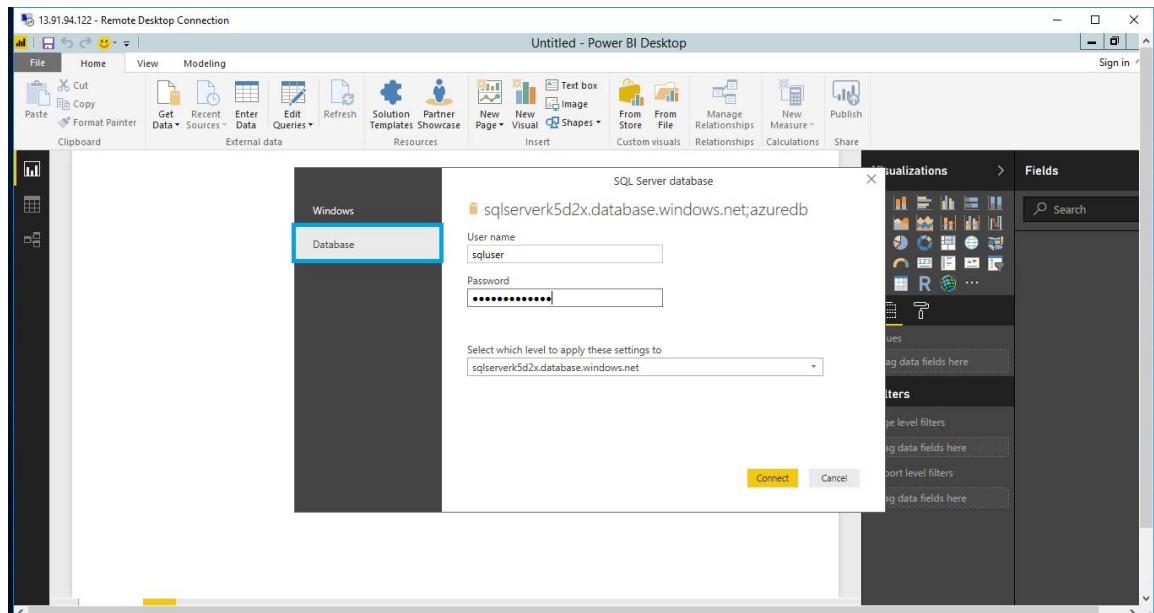


The screenshot shows the Power BI Desktop interface with the title bar 'Untitled - Power BI Desktop'. The ribbon menu includes File, Home, View, and Modeling. The 'Home' tab is selected, showing various data import and visualization tools. A report titled 'Building_Level_Summary_Report_Template_V0.3' is open, displaying configuration settings for a data source. It specifies the server as 'sqlserverk5d2x.database.windows.net' and the database as 'azuredb'. At the bottom right of the report window are 'Load' and 'Cancel' buttons.

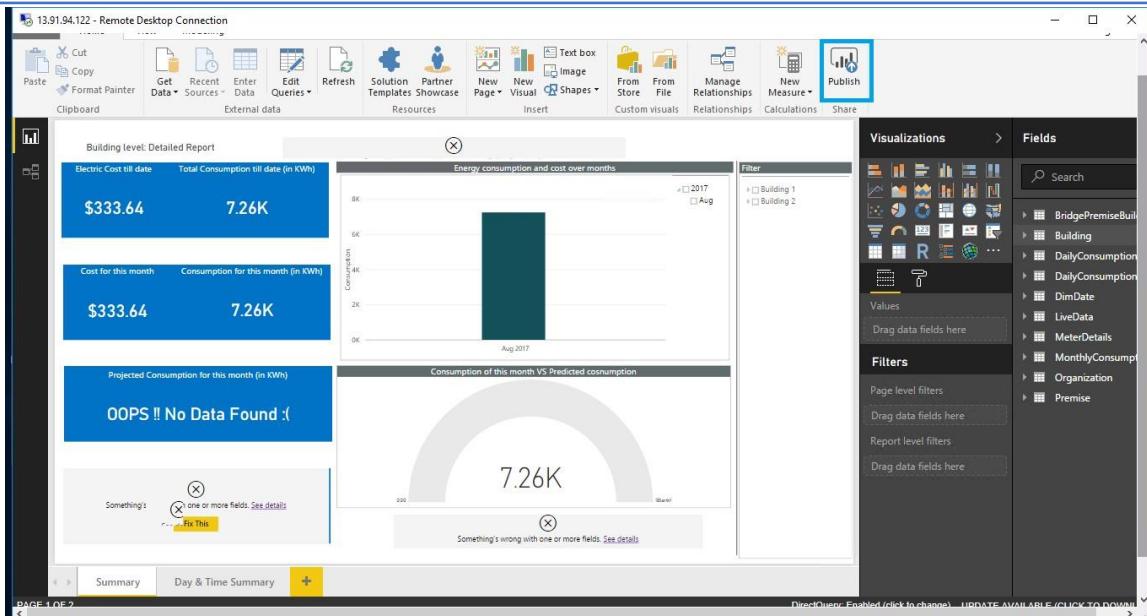
- Once you click on Load, the "Native Database Query" will appear, click on Run.



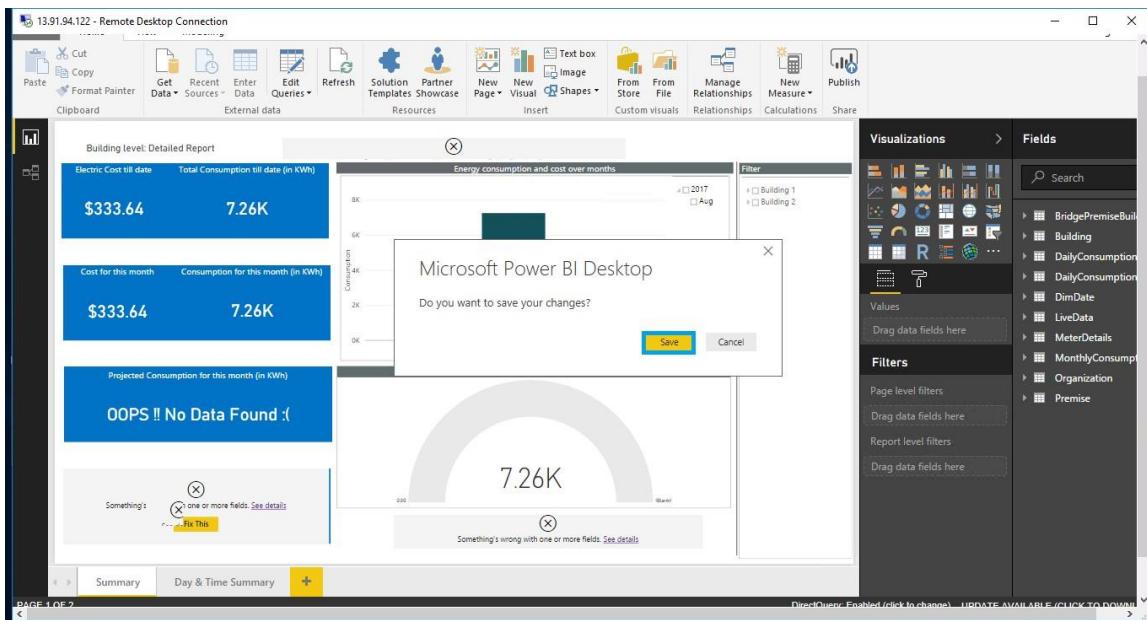
18. Select **Database** after connecting to the Azure SQL Server. Enter the login credentials of Azure database and click on **Connect**.



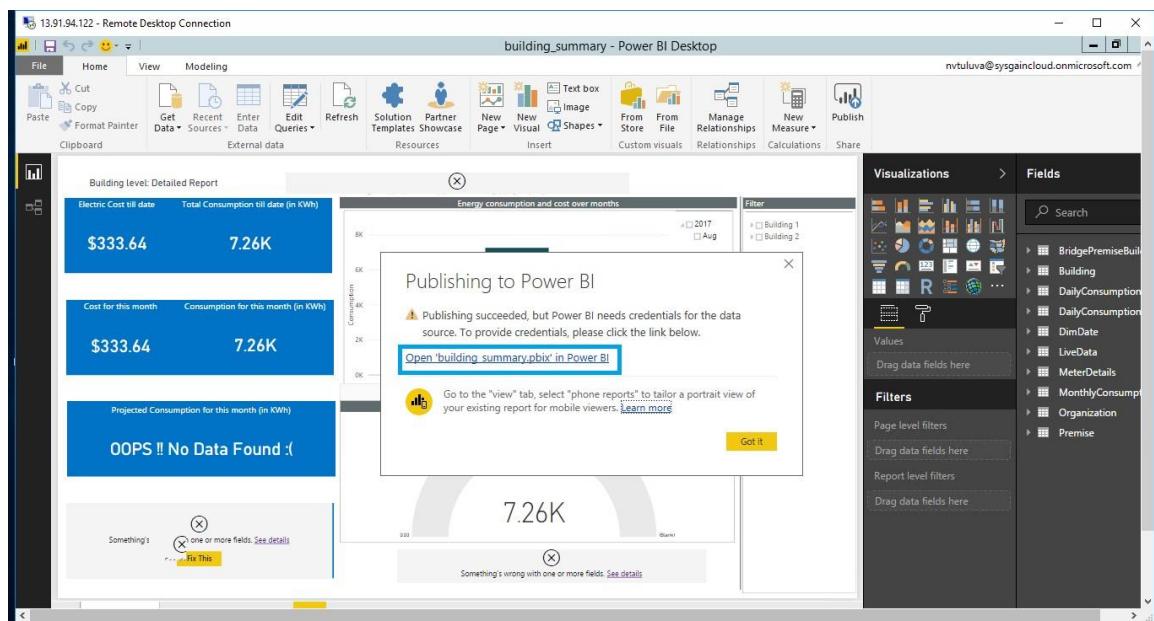
19. Click on **Publish**.



20. Save the changes.

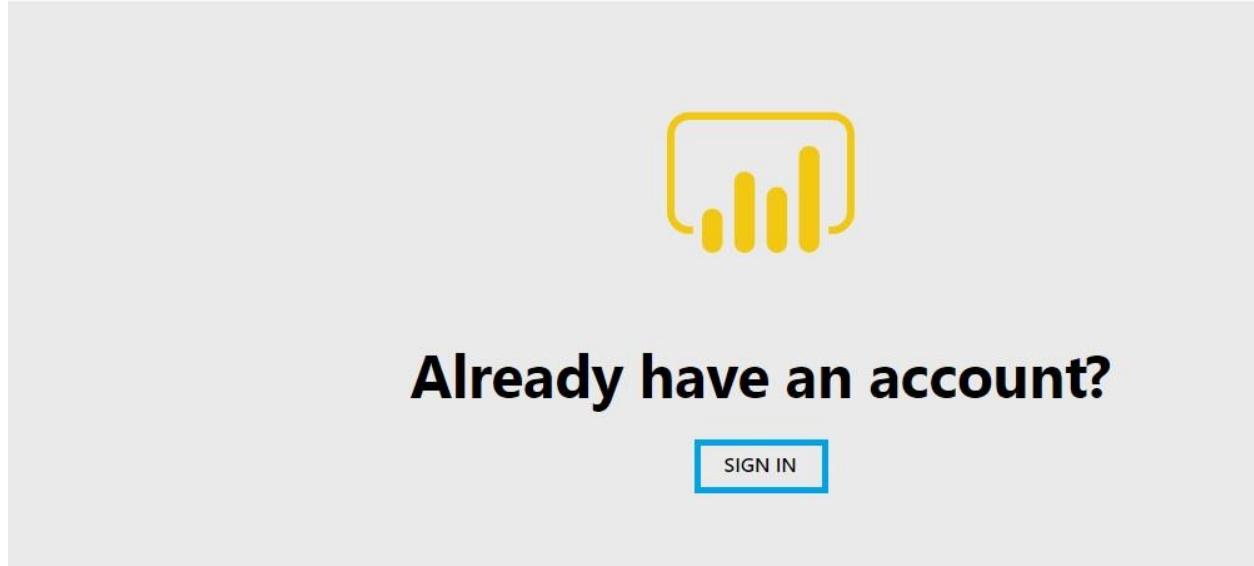


21. Click on the link as shown below, it will open in a web browser.

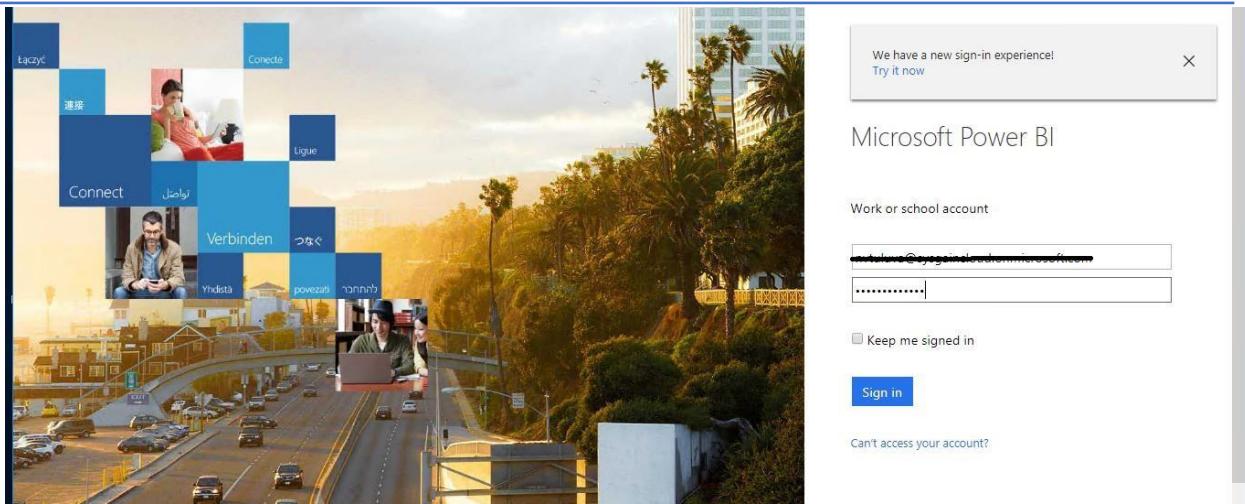


22. Sign in with the same credentials which were used to log to Power BI.

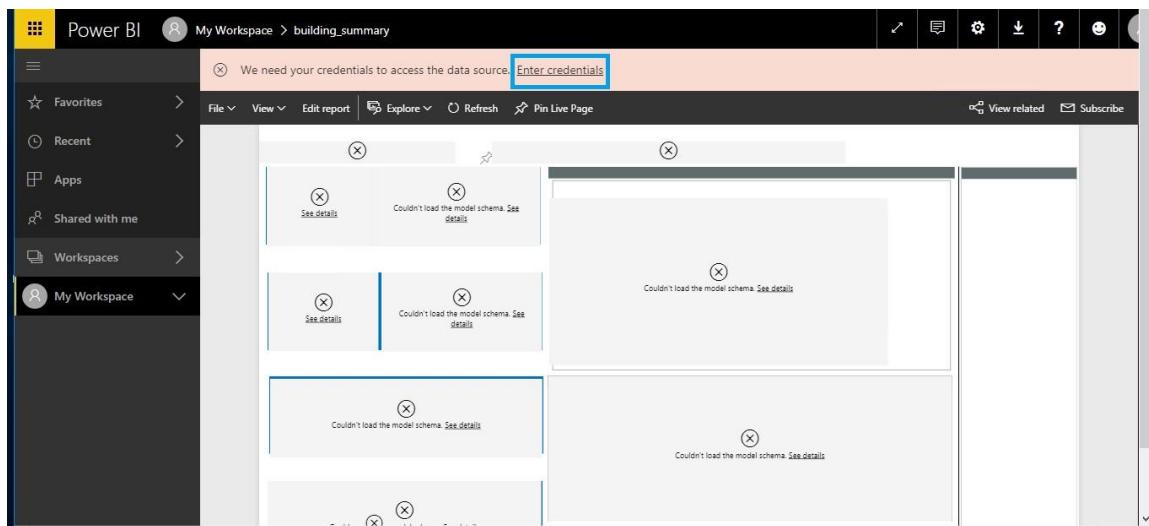
 Microsoft | Power BI



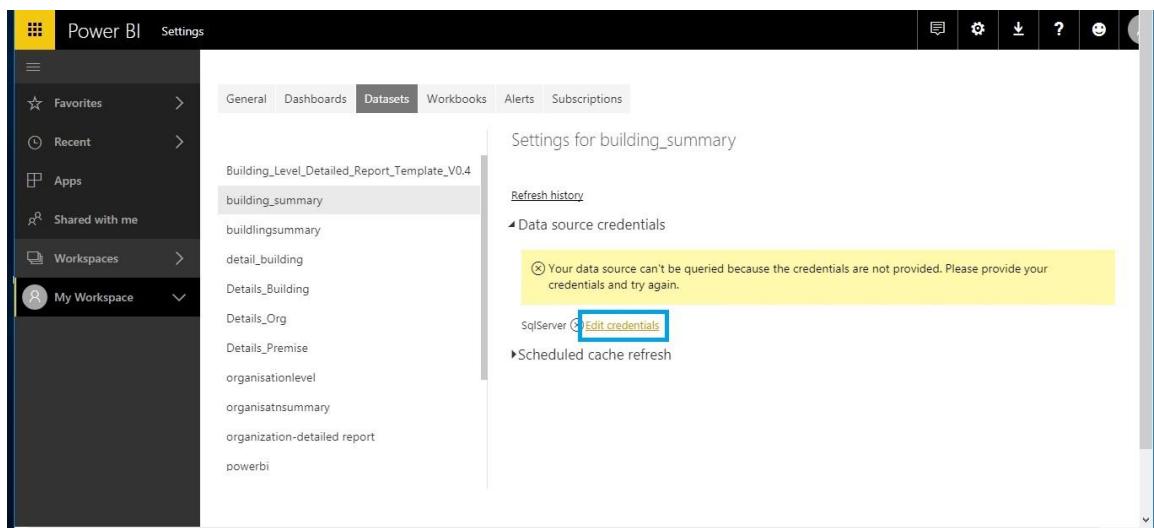
23. Enter the Power BI Credentials.



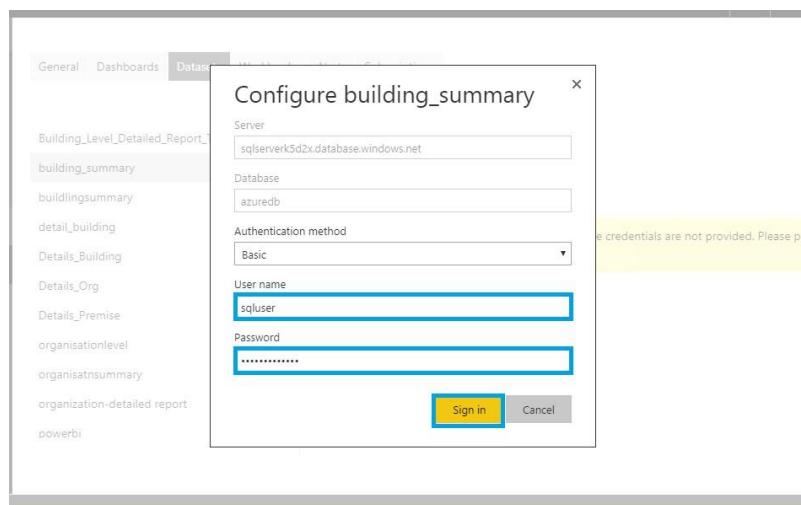
24. Click on **Enter credentials.**



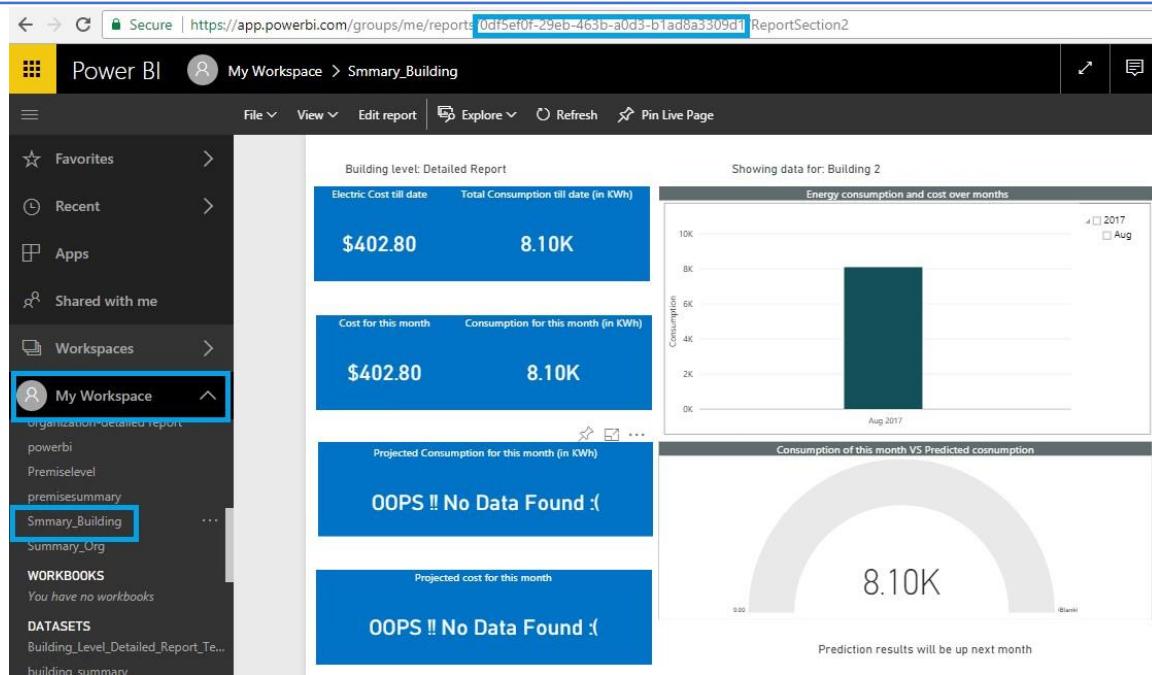
25. Click on **Edit credentials.**



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.



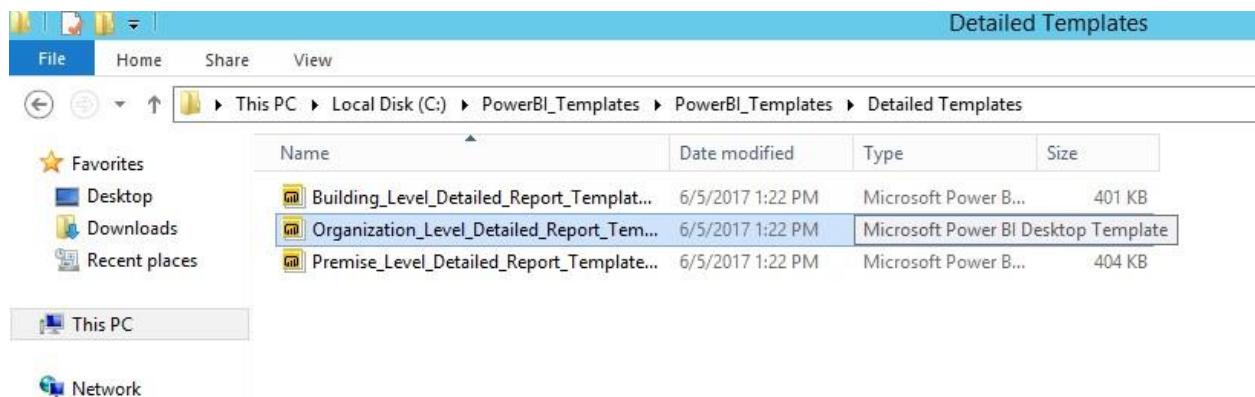
The screenshot shows a Power BI workspace titled "My Workspace > Summary_Building". The left sidebar lists "Favorites", "Recent", "Apps", "Shared with me", "Workspaces", and "My Workspace" (which is selected). Under "My Workspace", there are links for "organization-detailed-report", "powerbi", "Premiselevel", "premisesummary", "Summary_Building" (which is highlighted with a blue box), and "Summary_Org". The main area displays a "Building level: Detailed Report" with the following data:

- Electric Cost till date: \$402.80
- Total Consumption till date (in KWh): 8.10K
- Cost for this month: \$402.80
- Consumption for this month (in KWh): 8.10K
- Projected Consumption for this month (in KWh): OOPS !! No Data Found
- Projected cost for this month: OOPS !! No Data Found

On the right, there is a chart titled "Energy consumption and cost over months" showing consumption for Building 2 from August 2017 to August 2017. A gauge below it shows the "Consumption of this month VS Predicted consumption" at 8.10K.

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

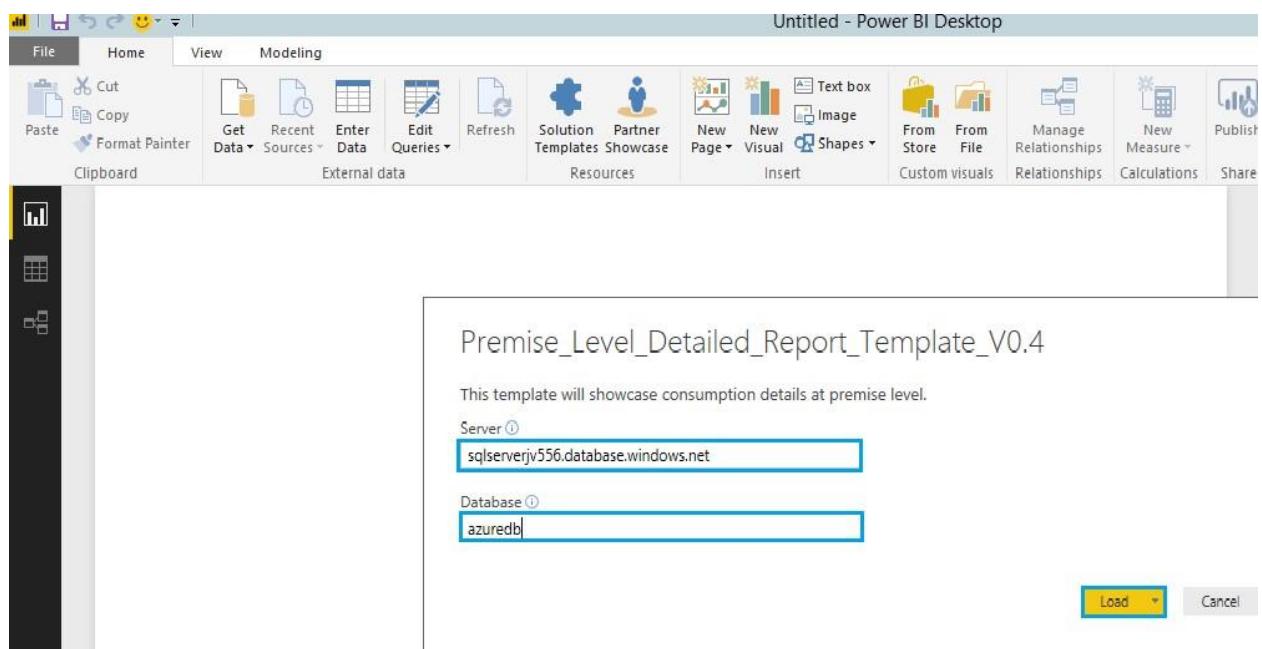
29. Navigate to **Power BI** templates and select **Detailed Template**



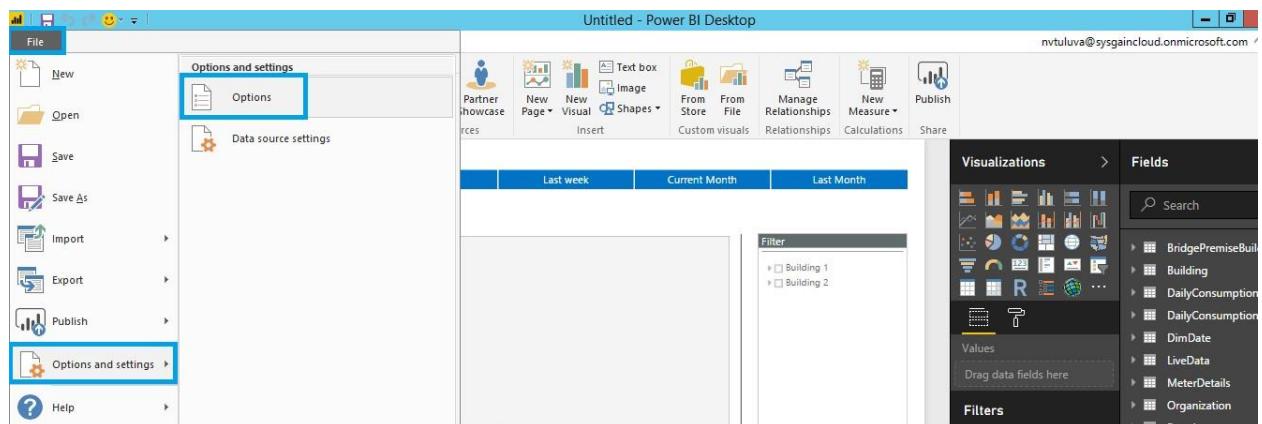
The screenshot shows the Windows File Explorer with the title bar "Detailed Templates". The left sidebar shows "Favorites", "Desktop", "Downloads", and "Recent places". The main area shows a list of files in the "Detailed Templates" folder:

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	404 KB
Premise_Level_Detailed_Report_Template...	6/5/2017 1:22 PM	Microsoft Power B...	404 KB

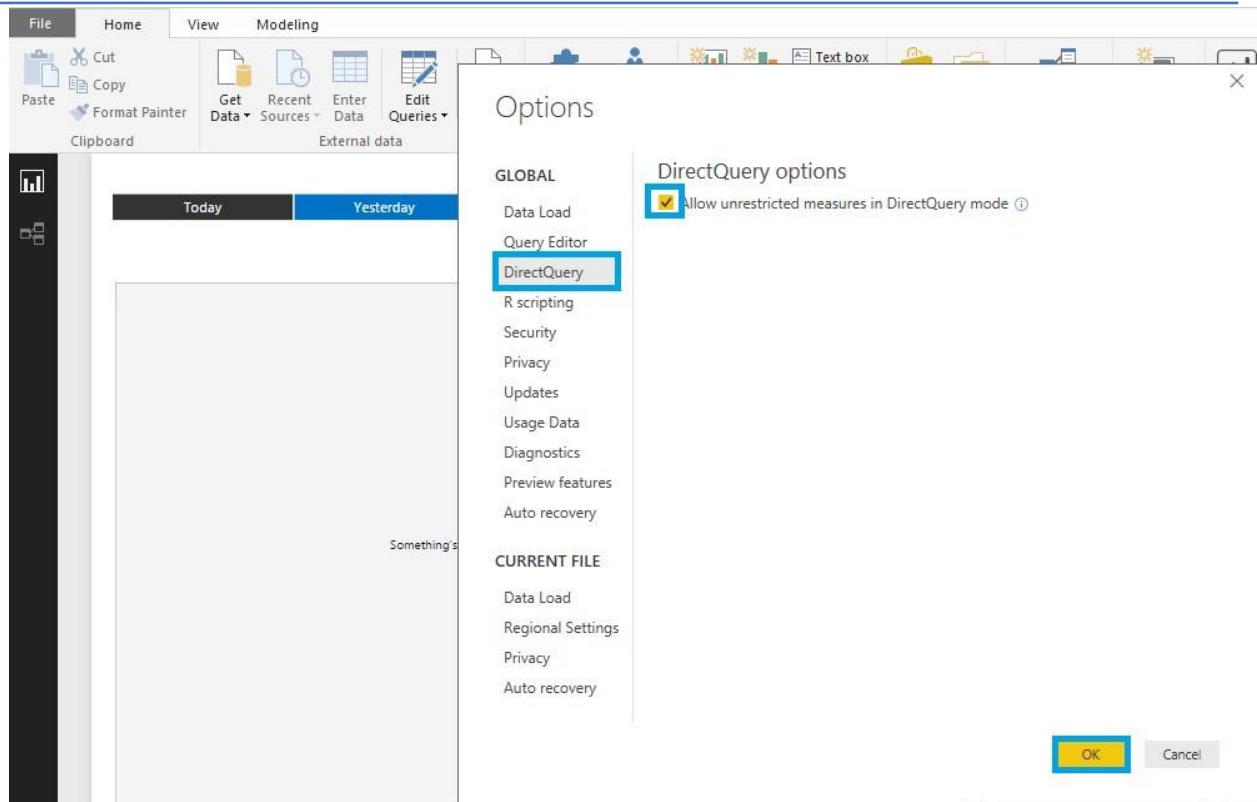
30. Enter the Azure SQL Server name with its password.



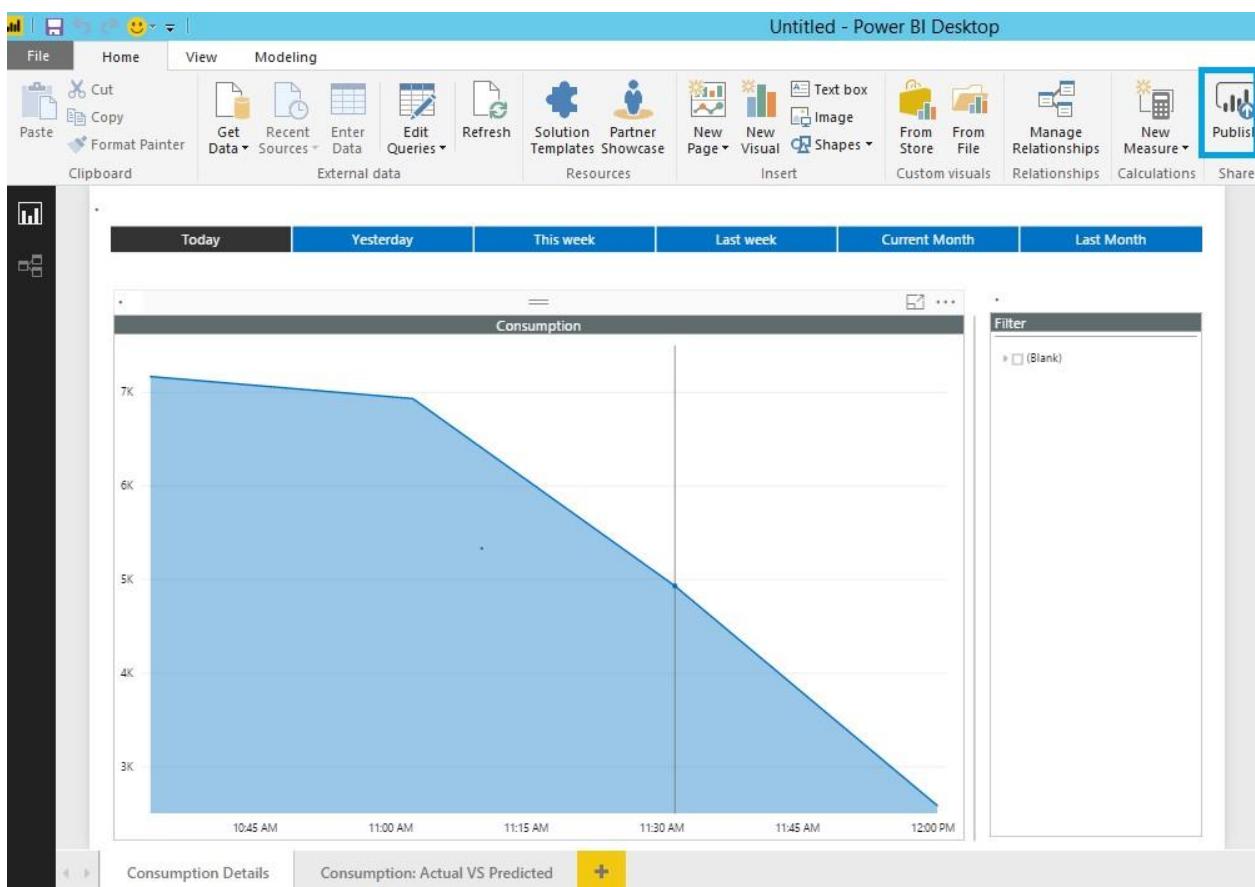
31. Navigate to **File > Options and Settings > Options**.



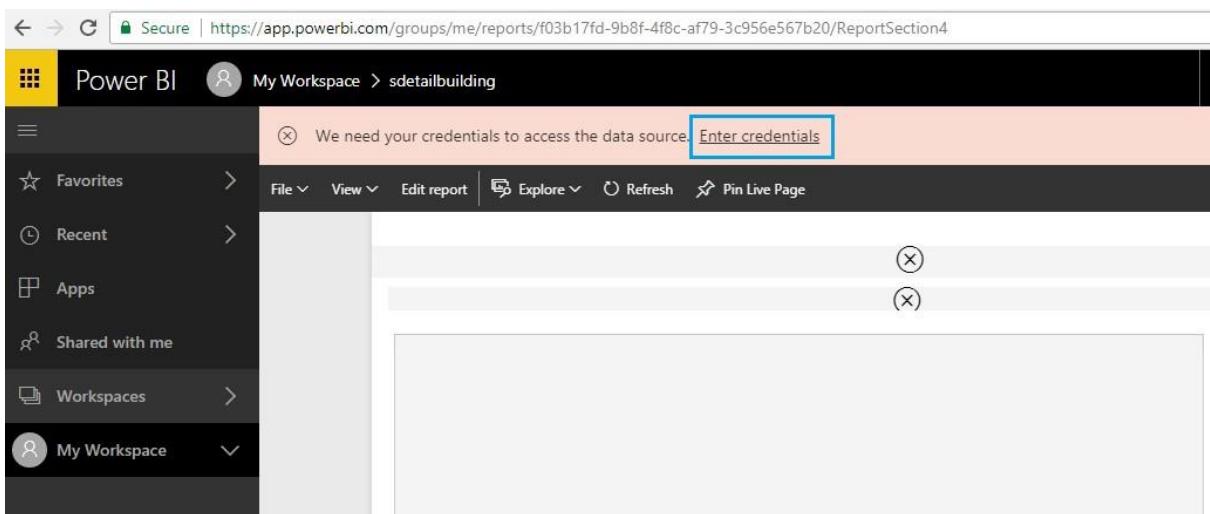
32. Select **DirectQuery** and then click on **OK**. Follow the same Process as done for the Summary template.



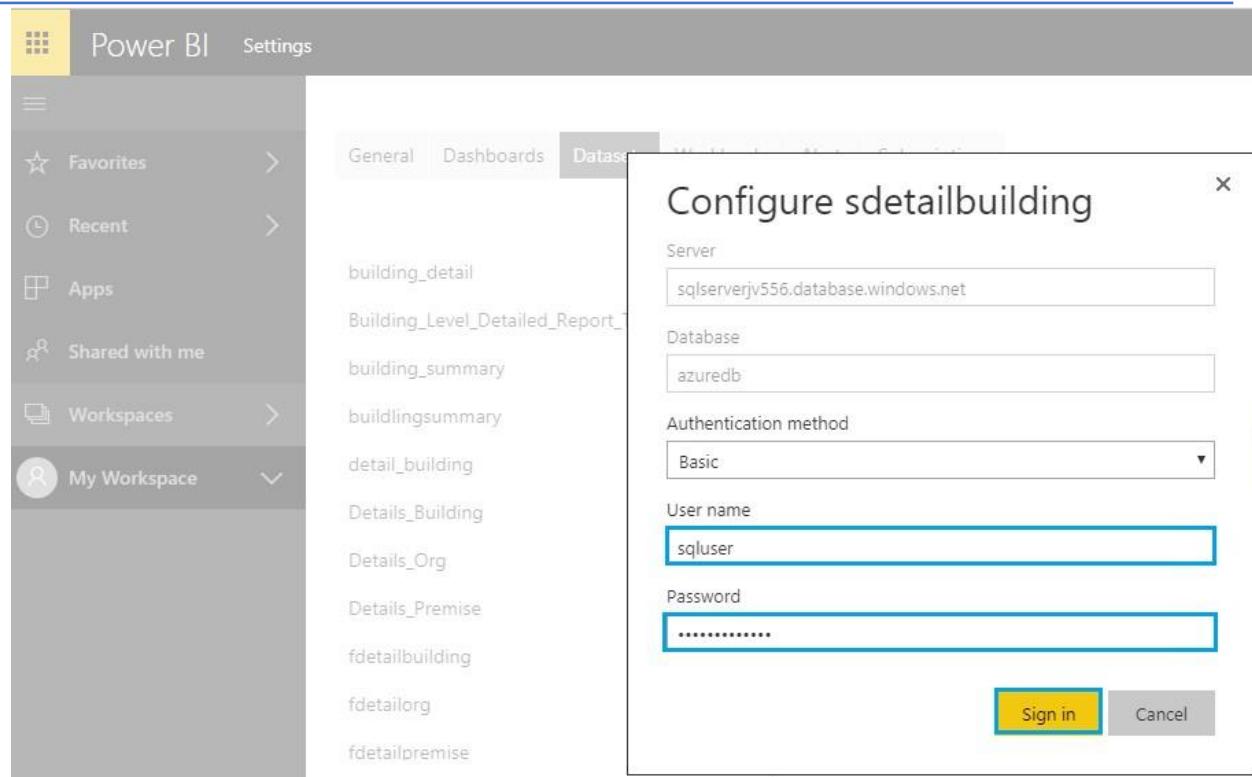
33. Click on **Publish** when you view the graph.



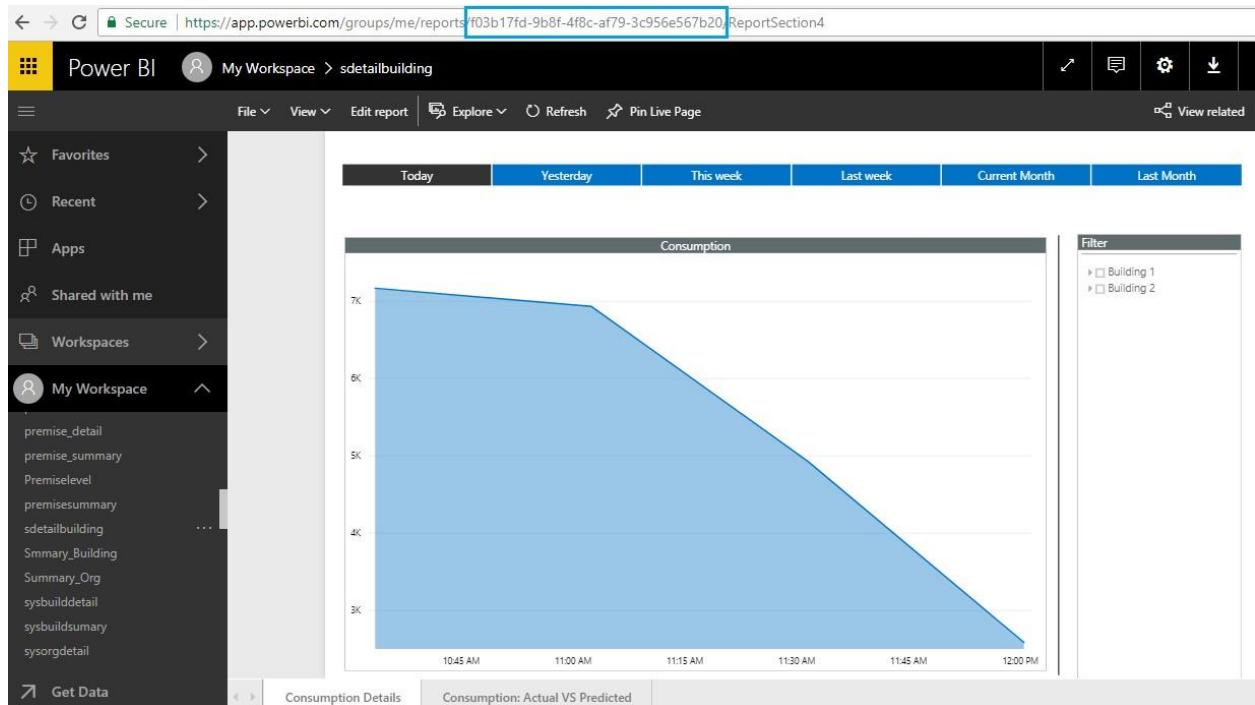
34. Click on **Enter credentials**.



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



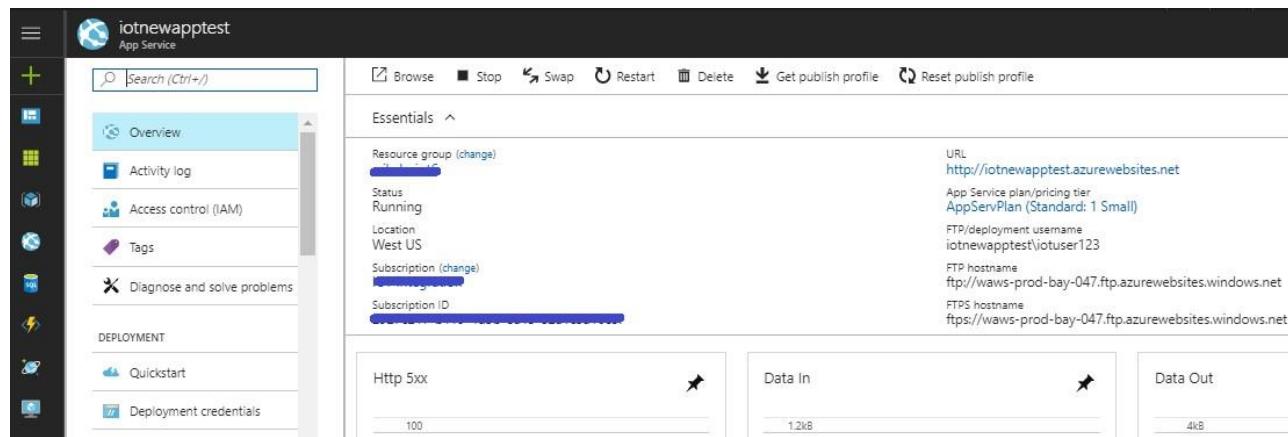
36. Copy the token from the URL after publishing each template and save it for further configuration in the web app.



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

11. Configuring and Accessing the Webapp

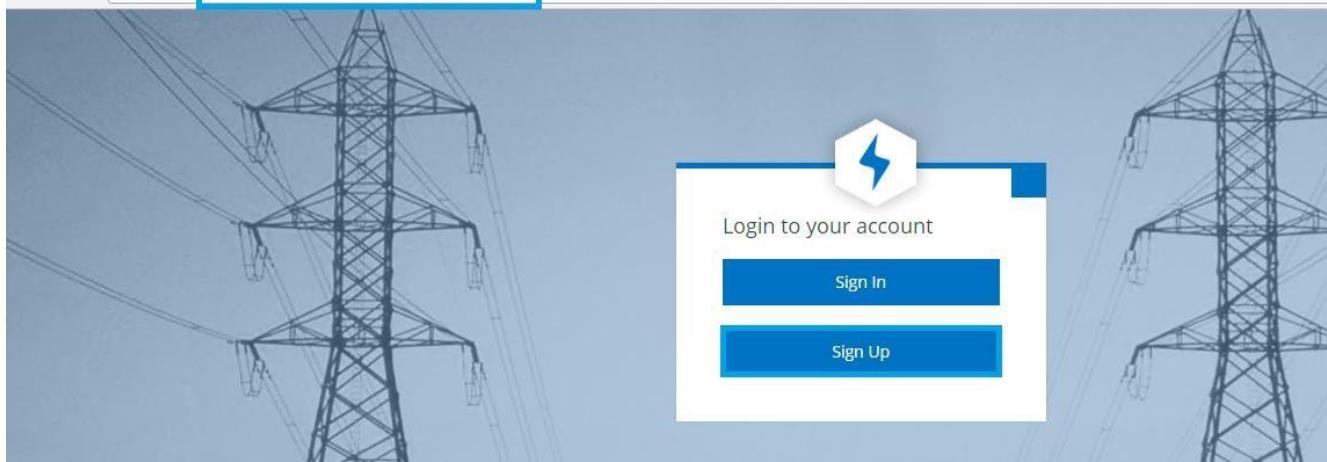
1. Go to the Web Application in the Resource Group and copy the address listed under "**URL**".



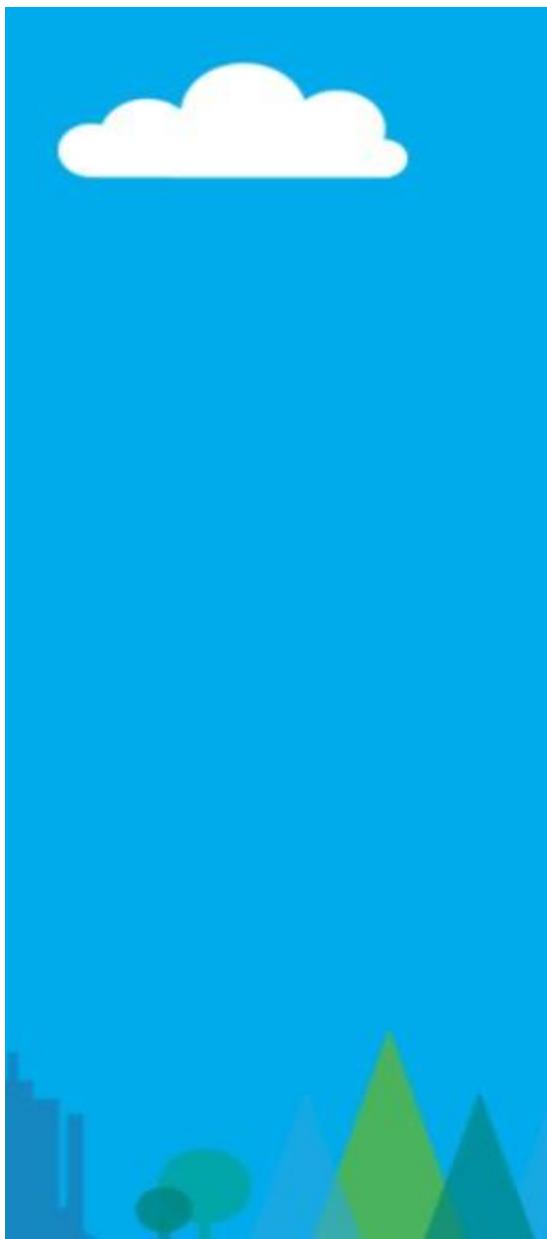
The screenshot shows the Azure portal's App Service configuration page for the application "iotnewappptest". The "Essentials" section displays the following details:

- Resource group (change)**: [REDACTED]
- Status**: Running
- Location**: West US
- Subscription (change)**: [REDACTED]
- Subscription ID**: [REDACTED]
- URL**: <http://iotnewappptest.azurewebsites.net>
- App Service plan/pricing tier**: AppServPlan (Standard: 1 Small)
- FTP/deployment username**: iotnewappptest\jotuser123
- FTP hostname**: ftp://waws-prod-bay-047.ftp.azurewebsites.windows.net
- FTPS hostname**: https://waws-prod-bay-047.ftp.azurewebsites.windows.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

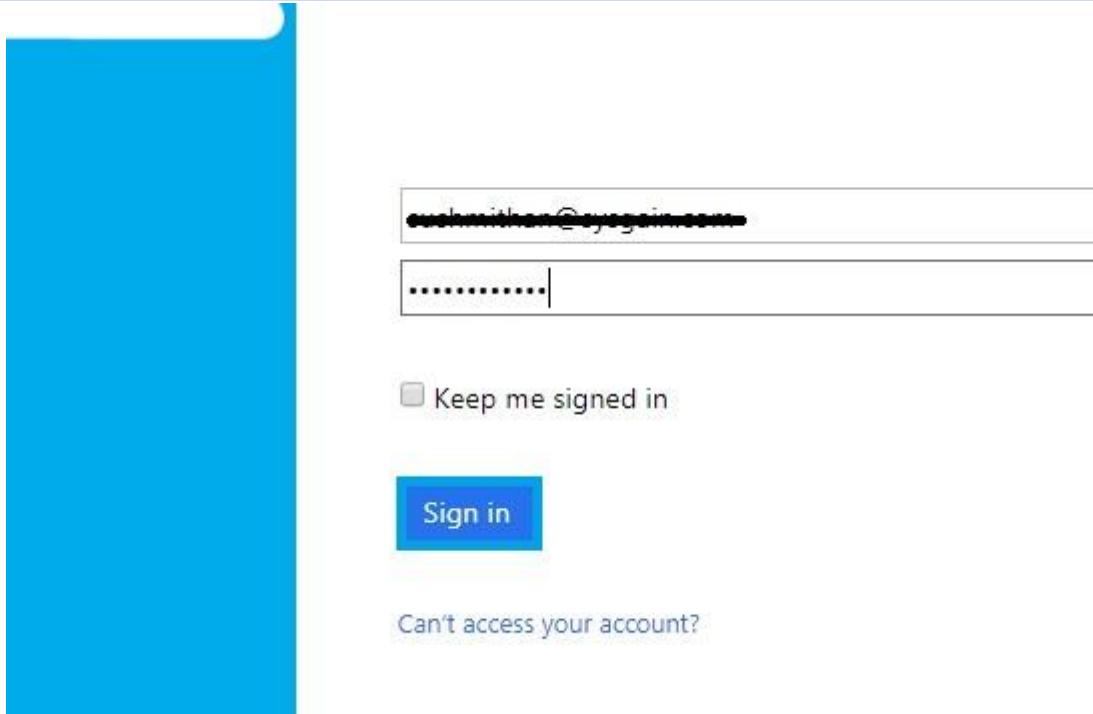
Display Name

Country/Region
 ▾

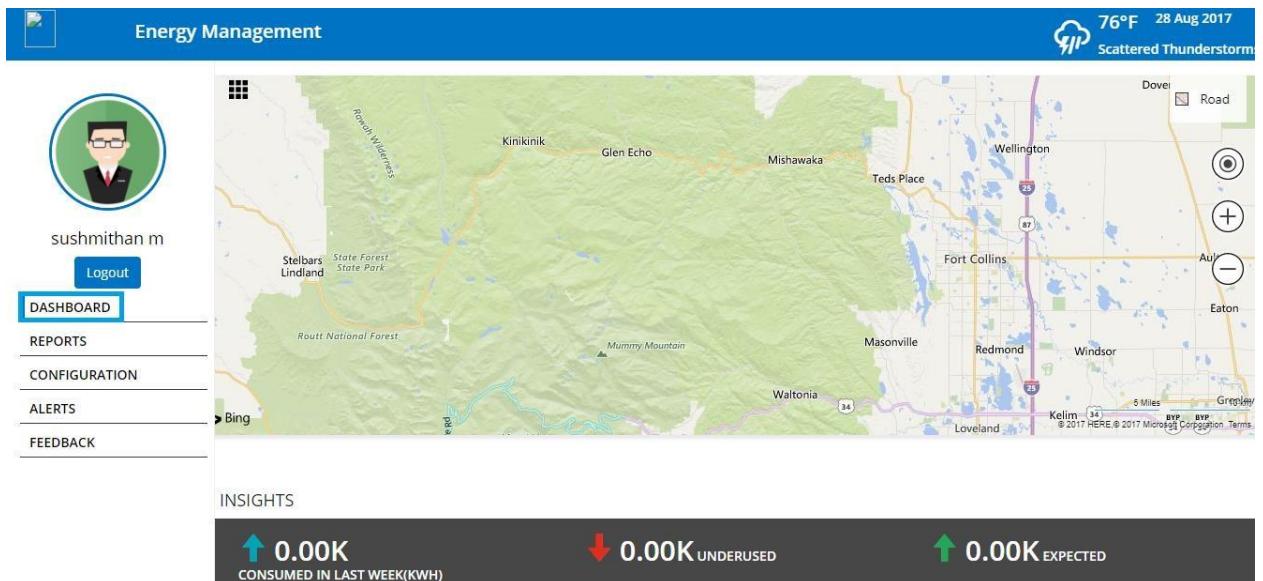
City

Activate Windows
Go to Settings to activate Windows.

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



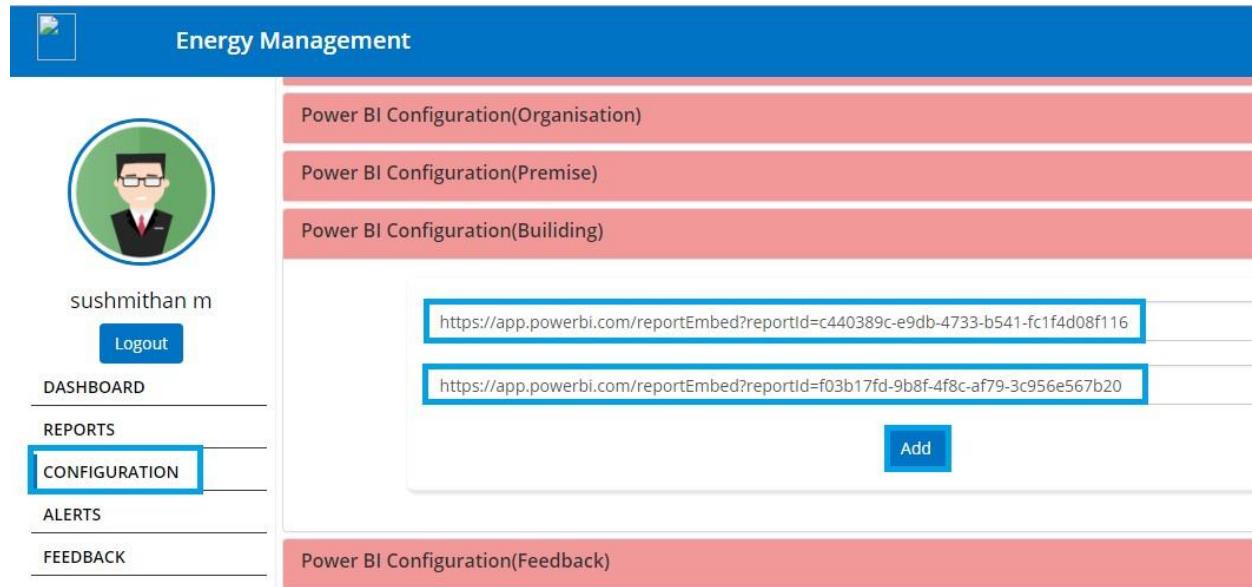
5. Once in the web app, you can view the **Dashboard** as shown below.



6. To configure the Power BI (**Building**), make the URL by using the Power BI tokens in the below format:

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

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

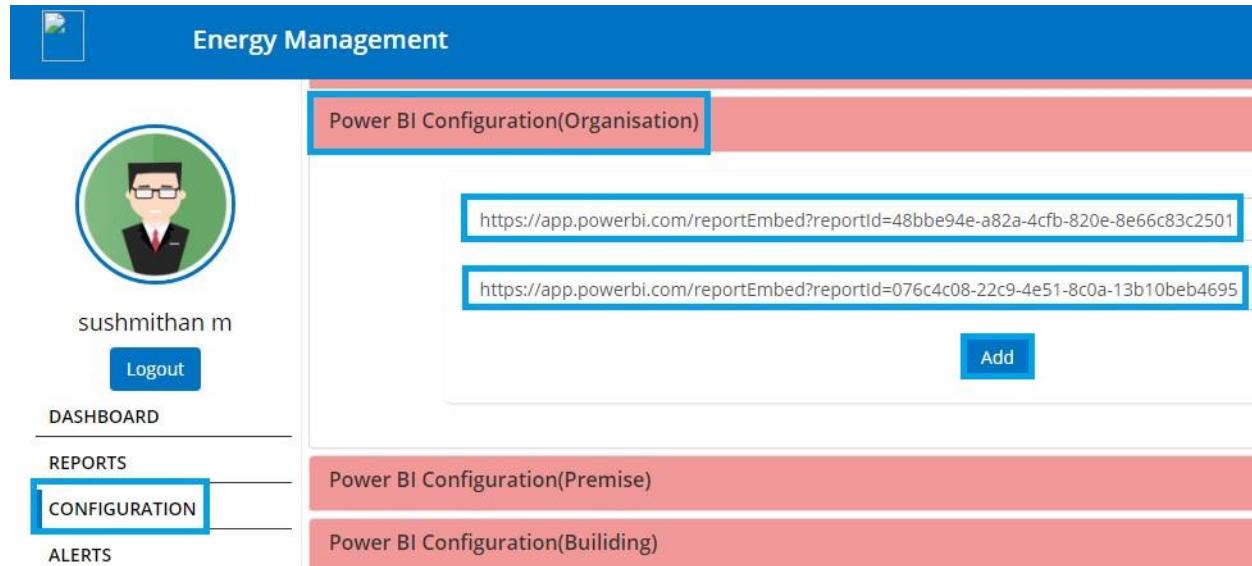


The screenshot shows the 'Energy Management' application interface. On the left, there is a sidebar with a user profile picture of a man in a suit, the name 'sushmithan m', and a 'Logout' button. Below this are menu options: DASHBOARD, REPORTS, **CONFIGURATION**, ALERTS, and FEEDBACK. The 'CONFIGURATION' option is highlighted with a blue border. The main content area has four red tabs: 'Power BI Configuration(Organisation)', 'Power BI Configuration(Premise)', 'Power BI Configuration(Building)', and 'Power BI Configuration(Feedback)'. Under 'Power BI Configuration(Organisation)', two URLs are 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**.

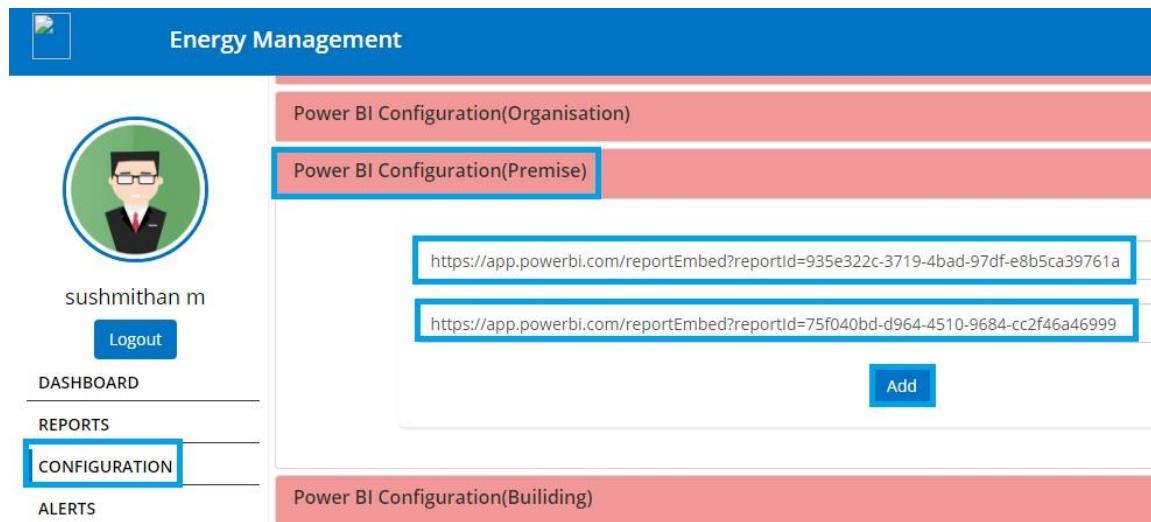


This screenshot shows the same 'Energy Management' application interface as the previous one, but with different URLs listed under the 'Power BI Configuration(Organisation)' tab. The URLs are: <https://app.powerbi.com/reportEmbed?reportId=48bbe94e-a82a-4cfb-820e-8e66c83c2501> and <https://app.powerbi.com/reportEmbed?reportId=076c4c08-22c9-4e51-8c0a-13b10beb4695>. The 'CONFIGURATION' menu item is also highlighted with a blue border here.

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

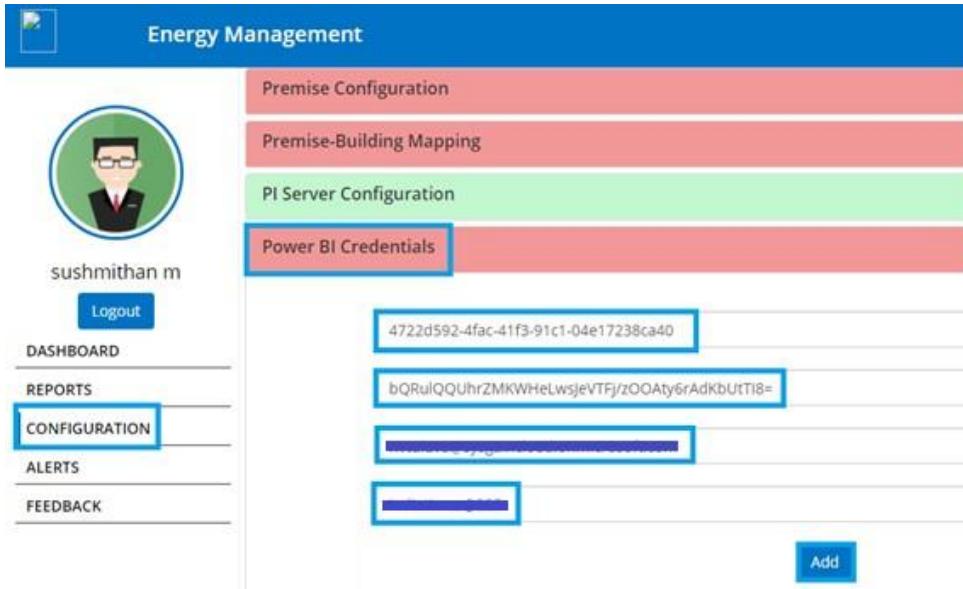
<https://app.powerbi.com/reportEmbed?reportId=<token>>

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 in a suit, 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 three red horizontal bars. The top bar contains the text 'Power BI Configuration(Organisation)'. The middle bar, which is highlighted with a blue border, contains the text 'Power BI Configuration(Premise)'. The bottom bar contains the text 'Power BI Configuration(Building)'. Under the 'Power BI Configuration(Premise)' bar, there are two URLs: <https://app.powerbi.com/reportEmbed?reportId=935e322c-3719-4bad-97df-e8b5ca39761a> and <https://app.powerbi.com/reportEmbed?reportId=75f040bd-d964-4510-9684-cc2f46a46999>. At the bottom right of the main content area is a blue 'Add' button.

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. On the left, there is a sidebar with a user profile picture of a man in a suit, the name 'sushmithan m', a 'Logout' button, and navigation links for 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted with a blue border), and 'FEEDBACK'. The main content area has a blue header bar. Below it, there are four horizontal bars. The first bar is pink and contains the text 'Premise Configuration'. The second bar is pink and contains the text 'Premise-Building Mapping'. The third bar is green and contains the text 'PI Server Configuration'. The fourth bar, which is highlighted with a blue border, contains the text 'Power BI Credentials'. Under the 'Power BI Credentials' bar, there are four URL-like fields, each containing a different string of characters. At the bottom right of the main content area is a blue 'Add' button.

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

Energy Management

ORGANIZATION SUMMARY



sushmithan m

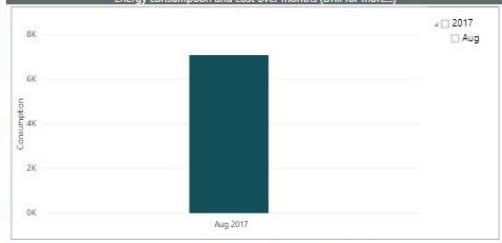
[Logout](#)

- [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 :(

Consumption and cost over months (Drill for more...)



Aug 2017

Aug

Consumption

8K
6K
4K
2K
0K

Consumption of this month VS Predicted consumption



7.09K

0.00 10.00

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

8K
7K
6K
5K
4K
3K
2K
1K

11:00 AM 11:30 AM 12:00 PM 12:30 PM

Filter

↳ (Blank)

Consumption Details
Consumption: Actual VS Predicted

Microsoft Power BI
1 of 2

12. Machine Learning Experiment

- 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 - Microsoft Azure

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

Microsoft Azure Resource groups > [REDACTED]

Overview (selected)

- Activity log
- Access control (IAM)
- Tags
- SETTINGS
 - Quickstart
 - Resource costs
 - Deployments
 - Policies
 - Properties
 - Locks
 - Automation script

Essentials

Subscription name (changed)	Deployments
IOT Integration	12 Succeeded
Subscription ID	[REDACTED]

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

77 items

NAME	TYPE	LOCATION
trendServer_OsDisk_1_e2ec285b58a345ae93...	Disk	South Central US
workspacePlan	Machine Learning web se...	South Central US
workspace	Machine Learning worksp...	South Central US
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 (selected)

- Activity log
- Access control (IAM)
- Tags
- SETTINGS
 - Quickstart
 - Resource costs
 - Deployments
 - Policies
 - Properties
 - Locks
 - Automation script
- MONITORING

Essentials

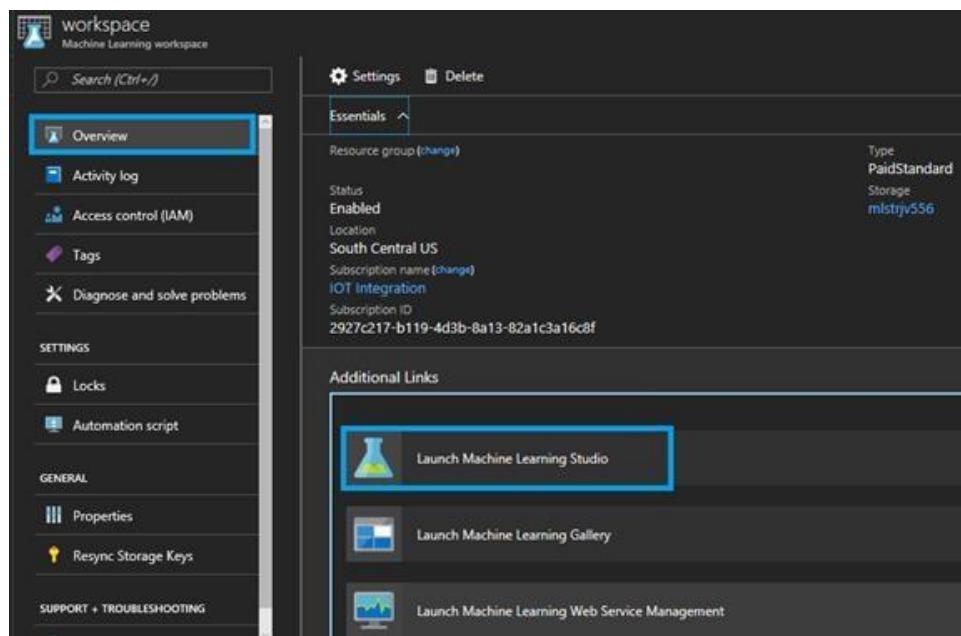
Subscription name (changed)	Deployments
IOT Integration	12 Succeeded
Subscription ID	2927c217-b119-4d3b-8a13-82a1c3a16cbf

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

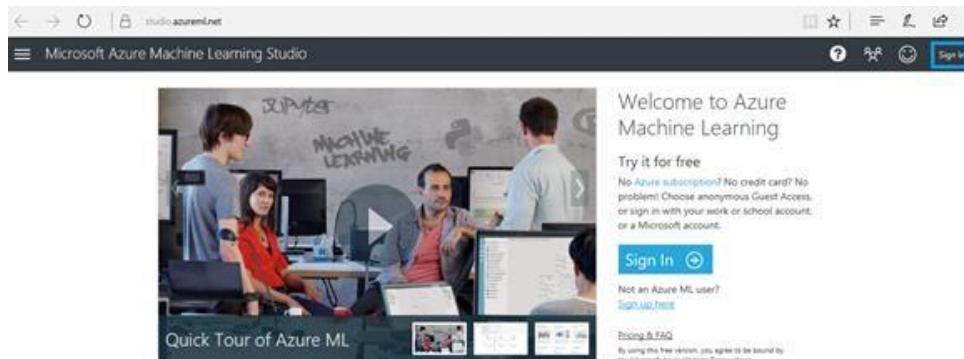
69 items

NAME	TYPE	LOCATION
splunkserver_disk2_b77ad5351b934e699fea...	Disk	South Central US
splunkserver_OsDisk_1_d4280ffaura4425a8e...	Disk	South Central US
trendServer_OsDisk_1_e2ec285b58a345ae93...	Disk	South Central US
workspacePlan	Machine Learning web se...	South Central US
workspace	Machine Learning worksp...	South Central US
adNfc	Network interface	South Central US

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



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

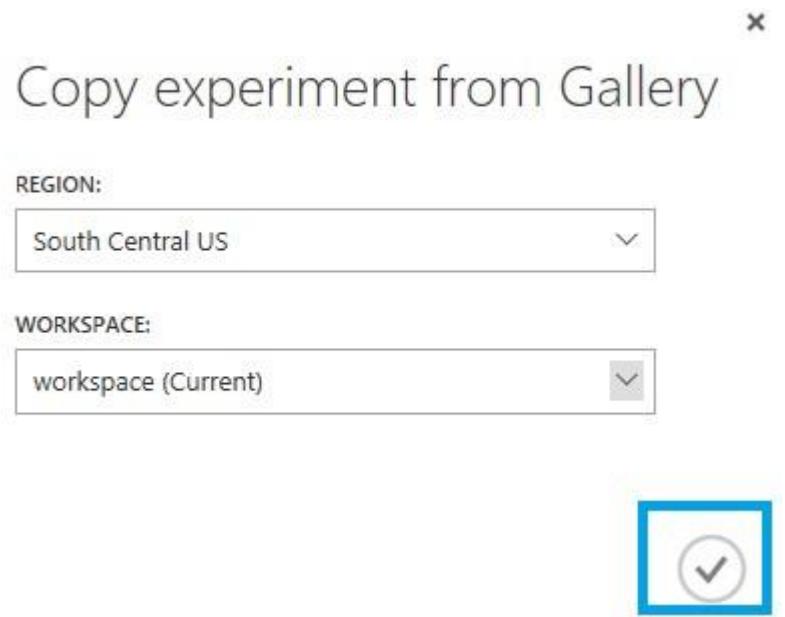


5. Open the below URL in a new browser and click on **Open in Studio**. This will launch the Experiment to the **workspace**.

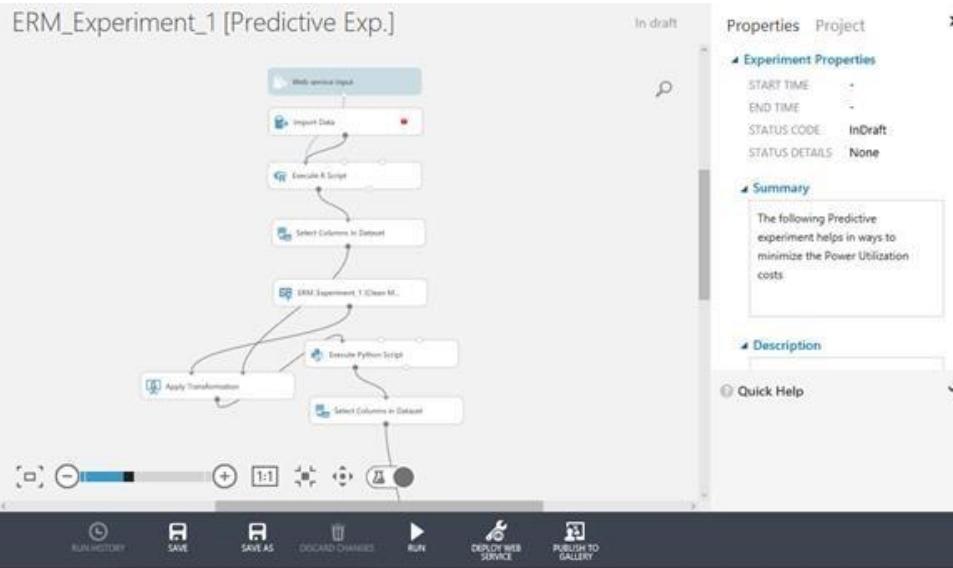
Path : <https://gallery.cortanaintelligence.com/Experiment/ERM-Experiment-1-Predictive-Exp>

The screenshot shows a web browser window with the address bar displaying 'gallery.cortanaintelligence.com/Experiment/ERM-Experiment-1-Predictive-Exp'. The main content area is titled 'Cortana Intelligence Gallery' and shows an experiment named 'ERM_Experiment_1 [Predictive Exp.]'. Below the title, it says 'Mohammed Khan - August 4, 2017' and has a 'Be the first to like.' button. A summary section states: 'The following Predictive experiment helps in ways to minimize the Power Utilization costs'. There is a 'Description:' section followed by a diagram illustrating a predictive model structure. At the bottom right is a blue button labeled 'Open in Studio'.

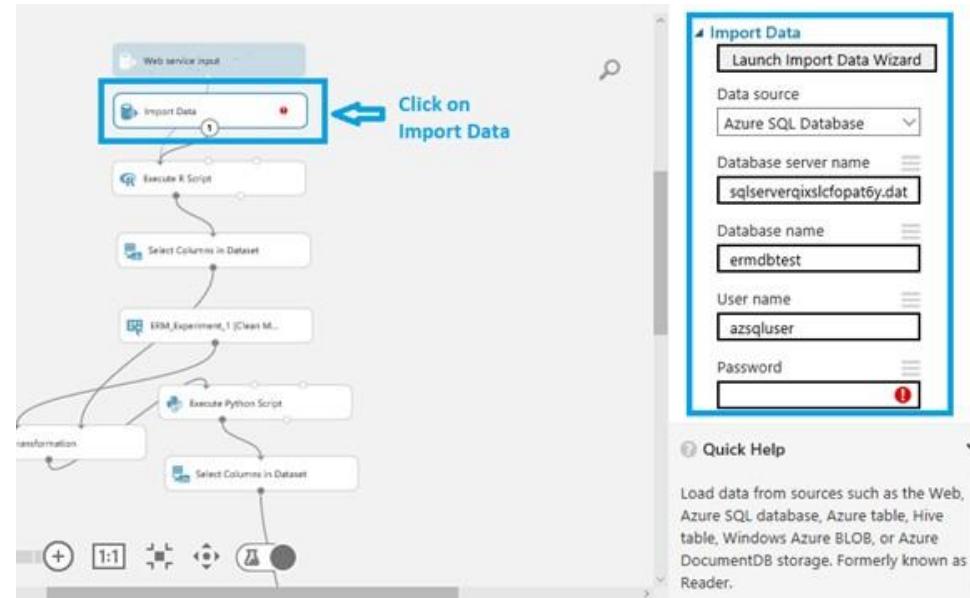
6. The below screen will appear in the new tab, click on the **check mark**.



7. The experiment will be downloaded to the workspace.



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



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

IMPORT DATA

x

Choose data source

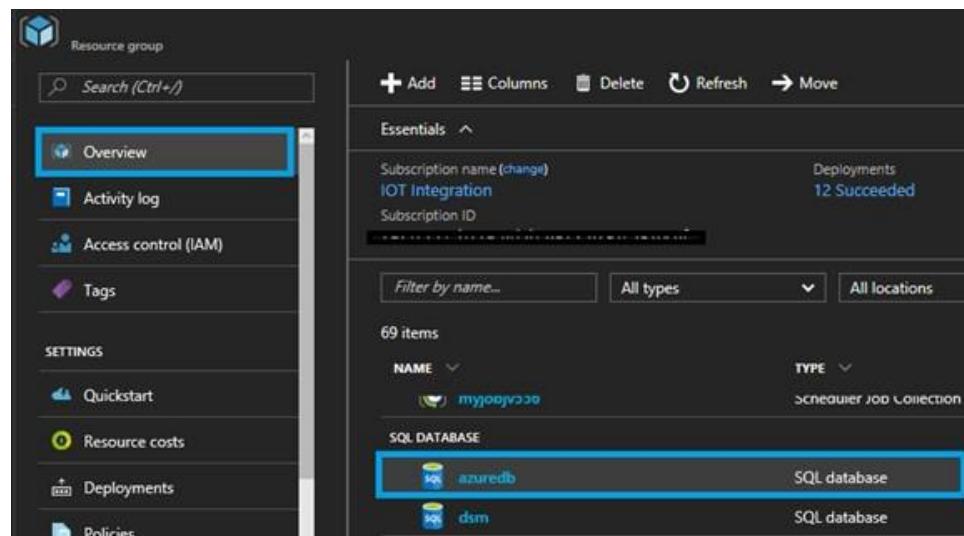
SOURCES

-  Web URL via HTTP
-  Hive Query
-  Azure SQL Database
-  Azure Table
-  Azure Blob Storage
-  Data Feed Provider
-  On-Premises SQL Database (Preview Feature)
-  Azure DocumentDB



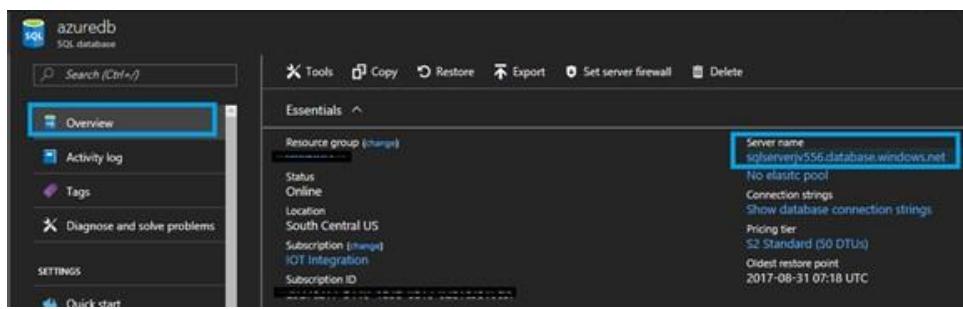
2 3

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



NAME	TYPE
azuredb	SQL database
dsm	SQL database

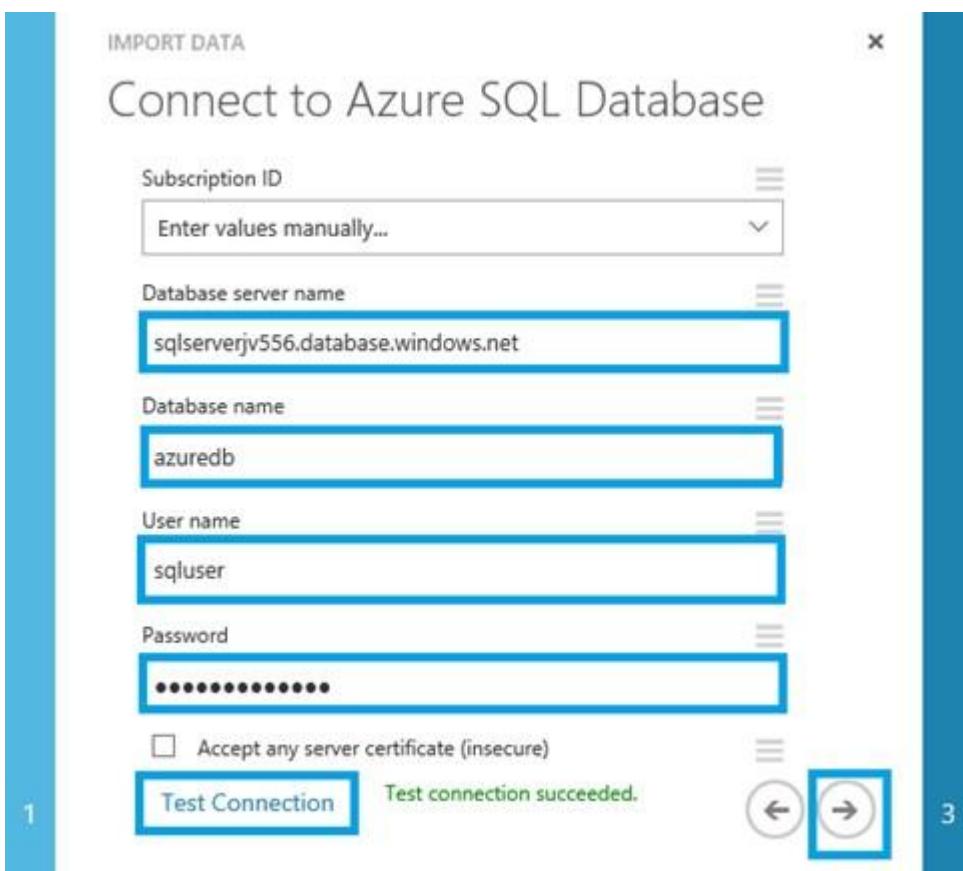
11. Open the Database **Server name**.



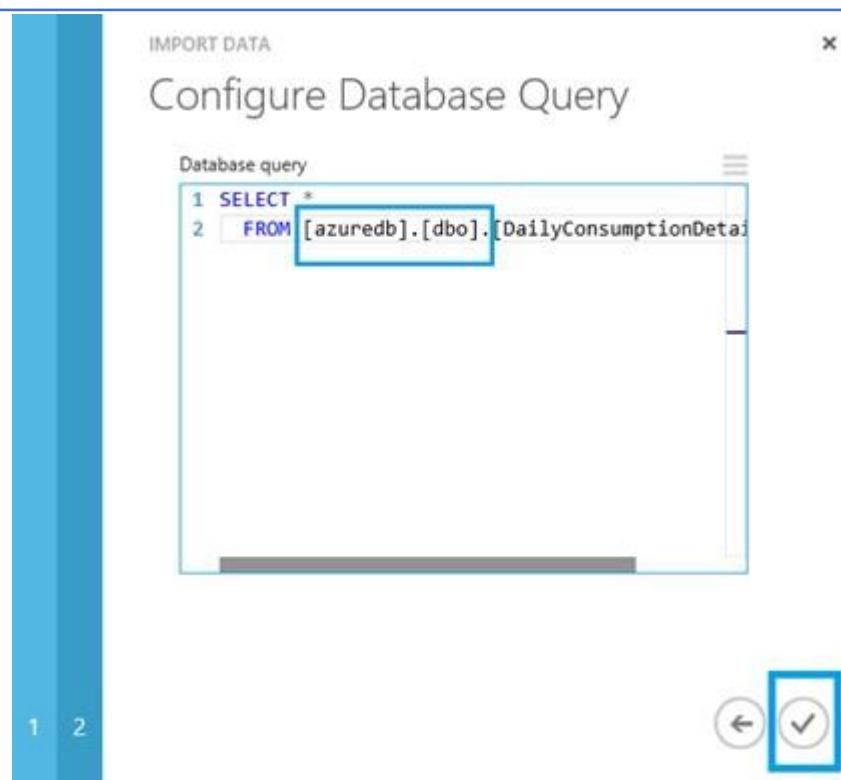
12. In the below screen, paste the **Database server name**.

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

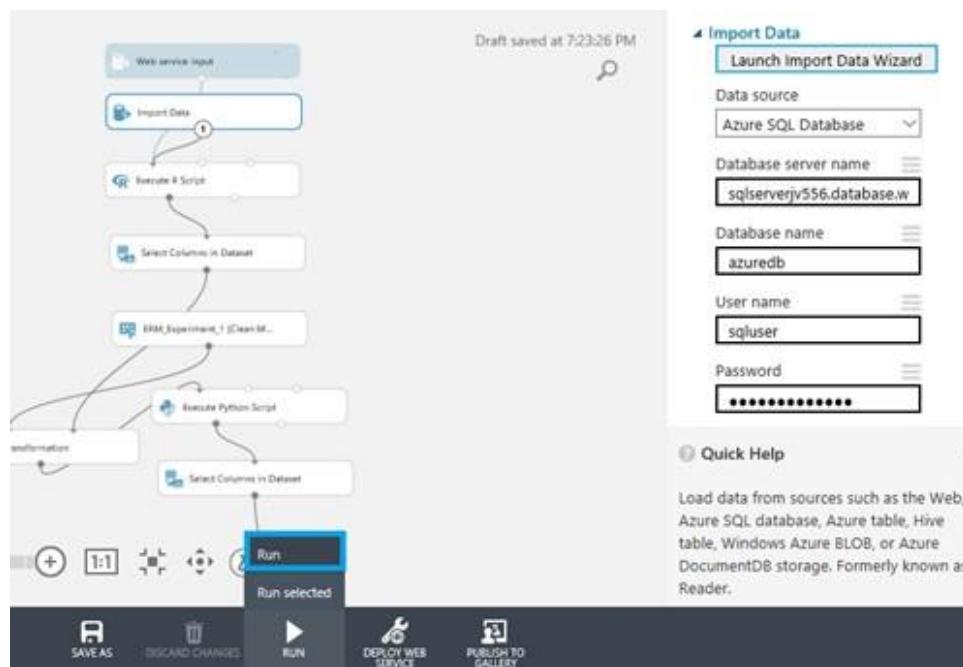
After the test connection succeeds, click on Next icon.



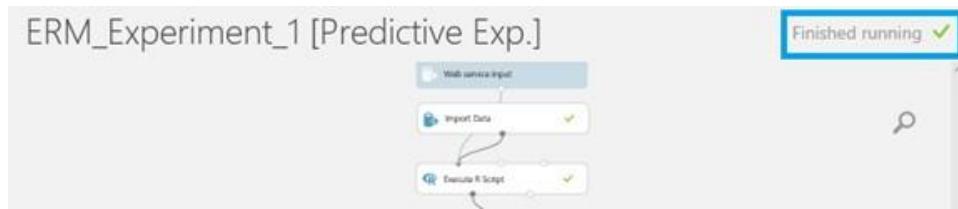
13. Replace the Database name with **azuredb** and click on the **check mark**.



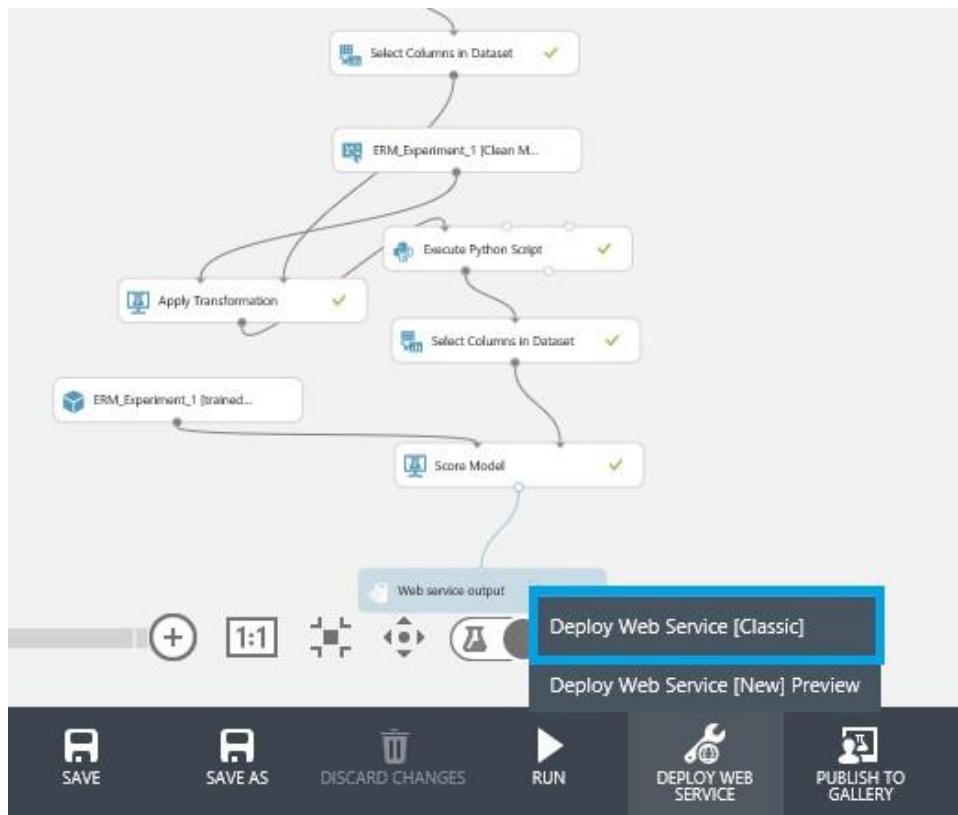
14. Once done, run the experiment by right clicking on **Run** from bottom of the below screen, and select **Run** from the dropdown menu.



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



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



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

[DASHBOARD](#) [CONFIGURATION](#)
[General](#) [New Web Services Experience preview](#)
[Published experiment](#)
[View snapshot](#) [View latest](#)
[Description](#)

No description provided for this web service.

API key

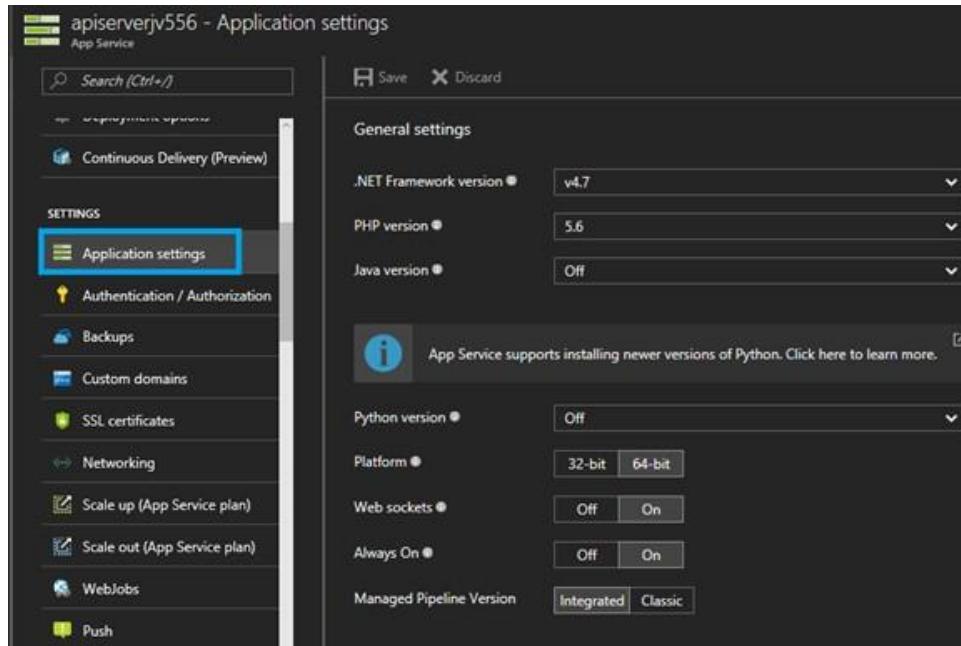
```
+n92PDuzx70O/tputyGUKRfts0Ul0AaCgbgmhZ03PjCxoIWww4J0Q7+tDaUEMESBIDFwxzgvbB+aOP0Lh5Ssag==
```

Default Endpoint

API HELP PAGE	TEST	APPS
REQUEST/RESPONSE	Test Test <small>preview</small>	 Excel 2013 or later
BATCH EXECUTION	Test <small>preview</small>	 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' page for an Azure App Service named 'apiserver'. 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 panel displays 'General settings' with 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 indicates that Python versions newer than Off can be installed.

21. Add

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

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

SETTINGS

- Application settings**
- Authentication / Authorization
- Backups
- Custom domains
- SSL certificates
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs

b2cSignInPolicyId	B2C_1_sipolicy2
b2cClientSecret	39iOK5g0LN\$rl7
b2cChangePasswordPolicy	B2C_1_cpasspolicy
EmailHost	iohost
EmailHostPort	25
EmailSender	noreply@gmail.com
EmailHostPassword	Password@1234
BlobStorageConnectionString	DefaultEndpointsProtocol=https;AccountName=webjo...
AzureMIAnomalyDetectionApiKey	+n92PDuzx70O/tpuyGUKRfts0U0AaCgbgmhZ03PjCxi...
AzureMIAnomalyDetectionApiUrl	https://ussouthcentral.services.azureml.net/workspaces/...

22. Restart the apiserver.

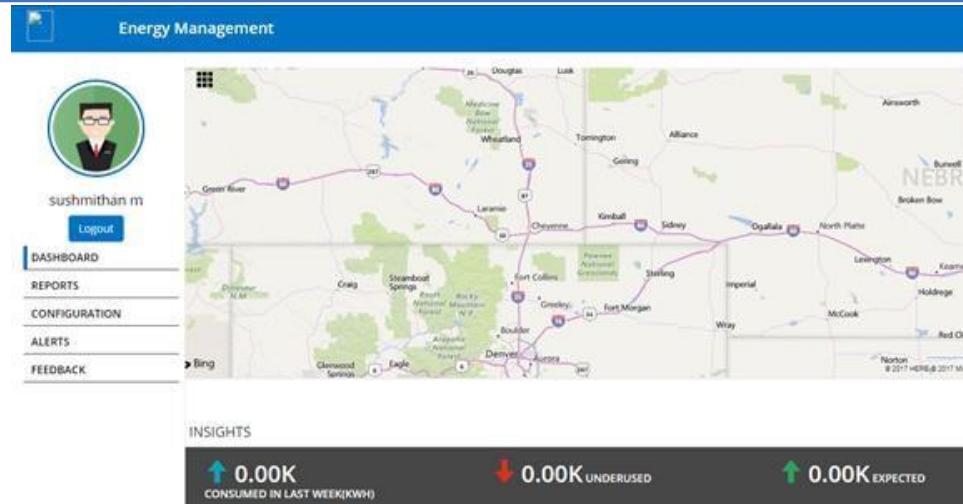
SETTINGS

- Application settings**
- Authentication / Authorization
- Backups
- Custom domains
- SSL certificates
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs

b2cSignInPolicyId	B2C_1_sipolicy2
b2cClientSecret	39iOK5g0LN\$rl7
b2cChangePasswordPolicy	B2C_1_cpasspolicy
EmailHost	iohost
EmailHostPort	25
EmailSender	noreply@gmail.com
EmailHostPassword	Password@1234
BlobStorageConnectionString	DefaultEndpointsProtocol=https;AccountName=webjo...
AzureMIAnomalyDetectionApiKey	+n92PDuzx70O/tpuyGUKRfts0U0AaCgbgmhZ03PjCxi...
AzureMIAnomalyDetectionApiUrl	https://ussouthcentral.services.azureml.net/workspaces/...

23. Login to the web application.



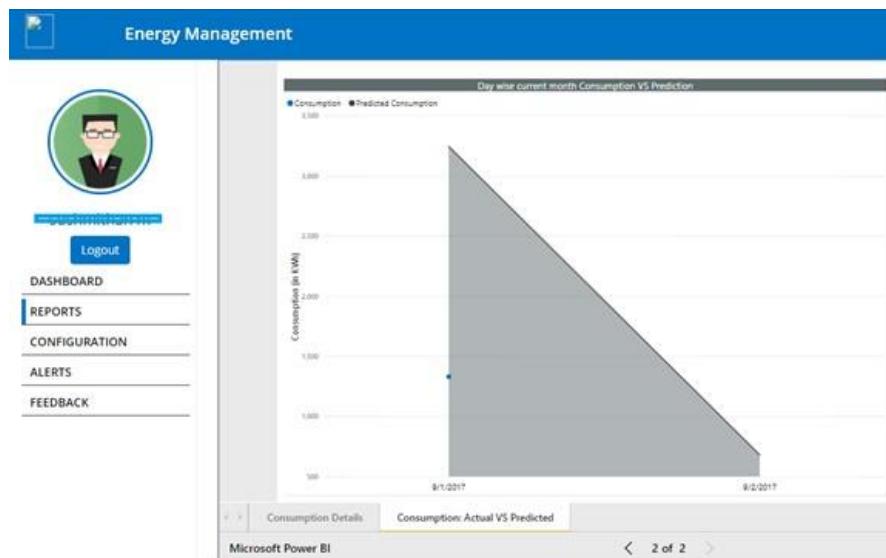


24. Navigate to **Azure ML Configuration** and add the **API Key** and **POST URL**.

Click on **Add**.

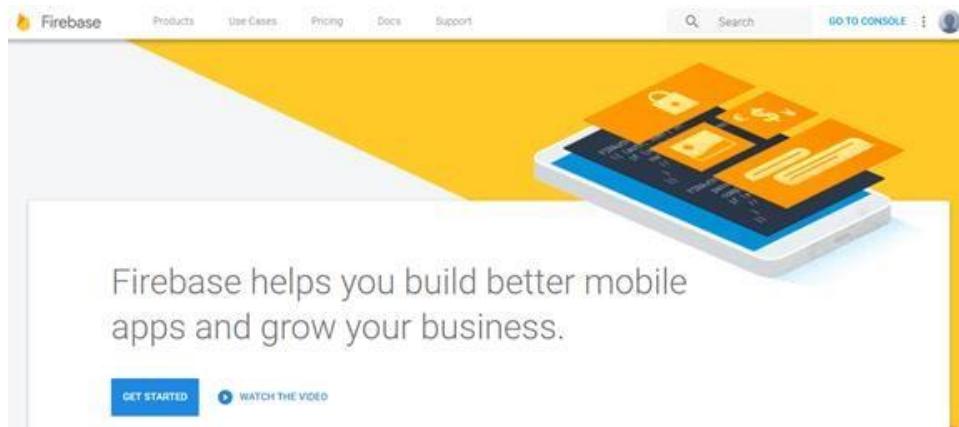


25. Click on **REPORTS** and click on **Consumption: Actual VS Predicted** of the bottom of the screen to view the Actual Vs Predicted graph.

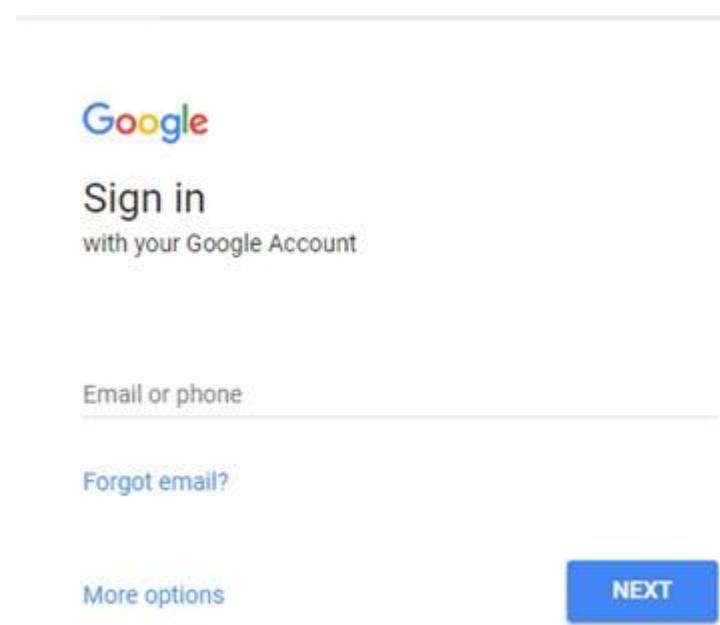


13. Firebase Configuration

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**.

Google
Sign in
with your Google Account

Email or phone

[Forgot email?](#)

[More options](#)

NEXT

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

Create a project X

Project name

Project ID ② edit

Country/region ②

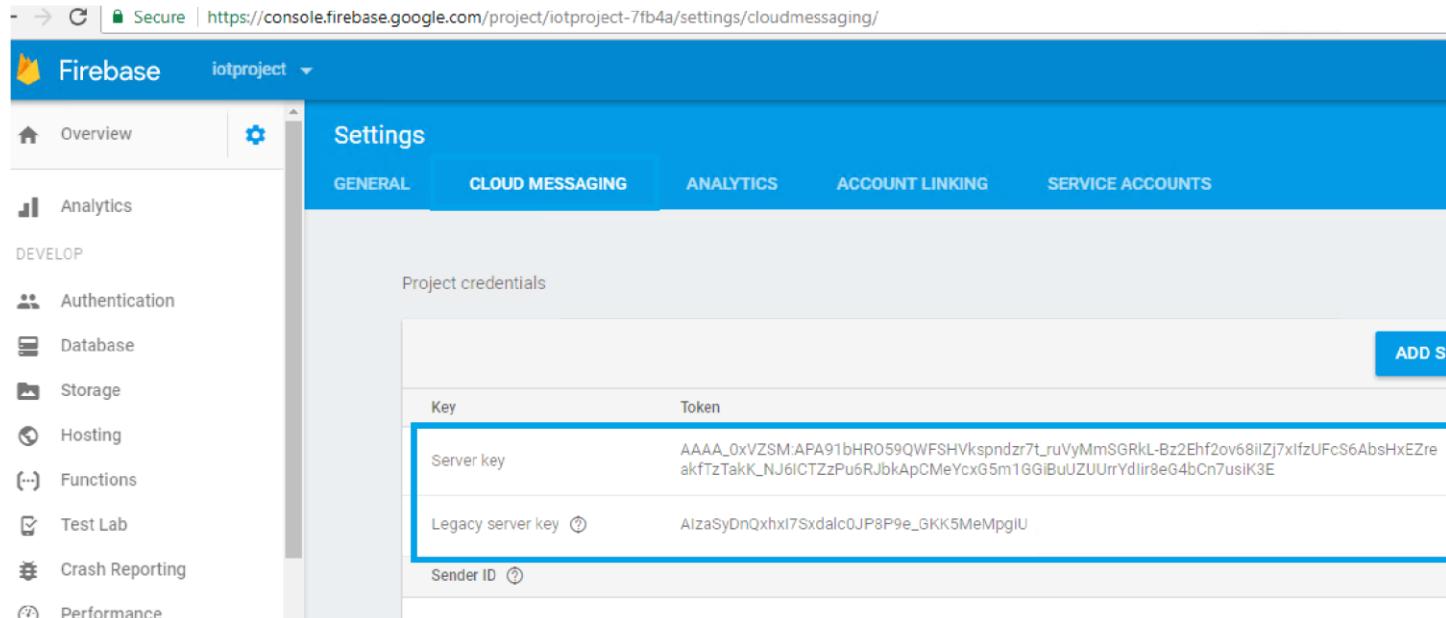
By default, your Analytics data will enhance other Firebase features and Google products. You can control how your analytics data is shared in your settings at anytime. [Learn more](#)

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 CREATE PROJECT

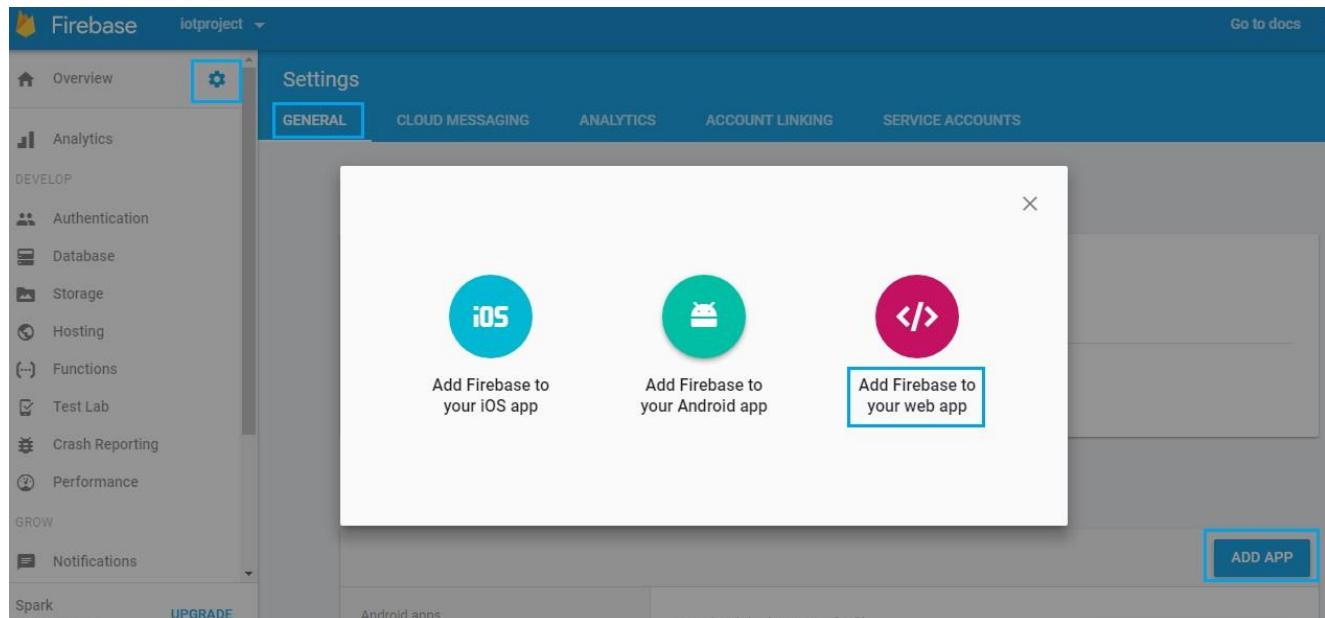
5. Navigate to **Settings > Project settings** > click on **CLOUD MESSAGIN**.
6. Save the **Server key** and **Legacy Server Key**.

Secure | https://console.firebaseio.google.com/project/iotproject-7fb4a/settings/cloudmessaging/



The screenshot shows the 'Cloud Messaging' tab selected in the Firebase 'Settings' interface. Under 'Project credentials', it lists two keys: 'Server key' and 'Legacy server key'. The 'Server key' row contains a long string of characters. Below these keys is a 'Sender ID' field with the value '1096497325347'. A blue box highlights the 'Server key' row.

- 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 'General' tab selected in the Firebase 'Settings' interface. A modal window is open, displaying three options: 'Add Firebase to your iOS app' (with an iOS icon), 'Add Firebase to your Android app' (with an Android icon), and 'Add Firebase to your web app' (with a code editor icon). The 'Add Firebase to your web app' button is highlighted with a blue box.

- 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 XCopy 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: "AIzaSyAbTdFA76Xo5THJRqIdRWLfDn63uYGHlo8",
    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:
  "AIzaSyAbTdFA76Xo5THJRqIdRWLfDn63uYGHlo8",
  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>
```

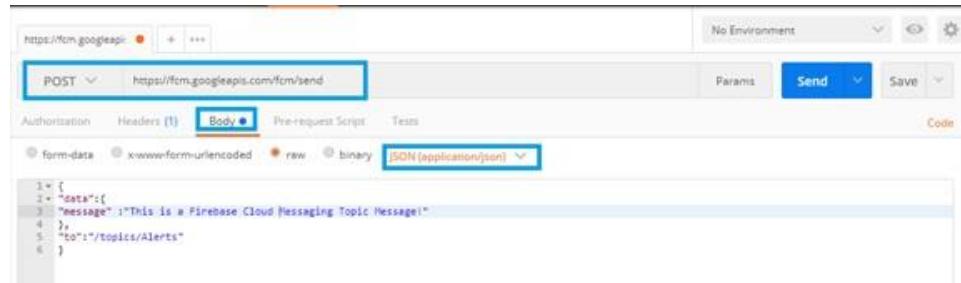
9. Open postman
 - Change the Params to **POST** and paste the below URL

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

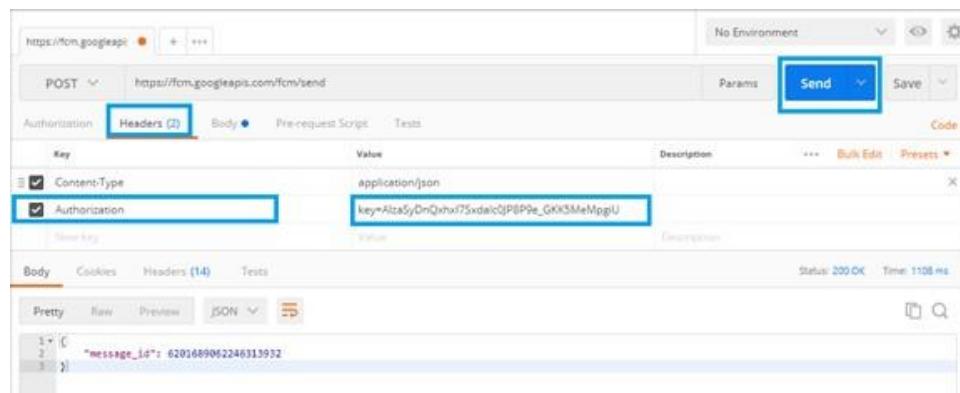
- Click on Body and enter the following:

```
{
  "data":{
    "message" :"This is a Firebase Cloud Messaging Topic Message!"
  },
  "to":"/topics/Alerts"
}
```

- Select the text to **Json**



- 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**.



- 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, there's a sidebar with a user profile icon, a 'Logout' button, and links for 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted in blue), 'ALERTS', and 'FEEDBACK'. The main content area has a red header bar with the title 'Firebase Configuration'. Below it, there are several input fields containing configuration details: a long string of characters, 'iotproject-7fb4a.firebaseioapp.com', 'https://iotproject-7fb4a.firebaseio.com', 'Storage Bucket', '1096497325347', and '/topics/Alerts'. At the bottom right, there are two green buttons: a larger one labeled 'Updated Firebase Configuration' and a smaller one below it labeled 'Configuration Updated'.

14. Restore Virtual Machines

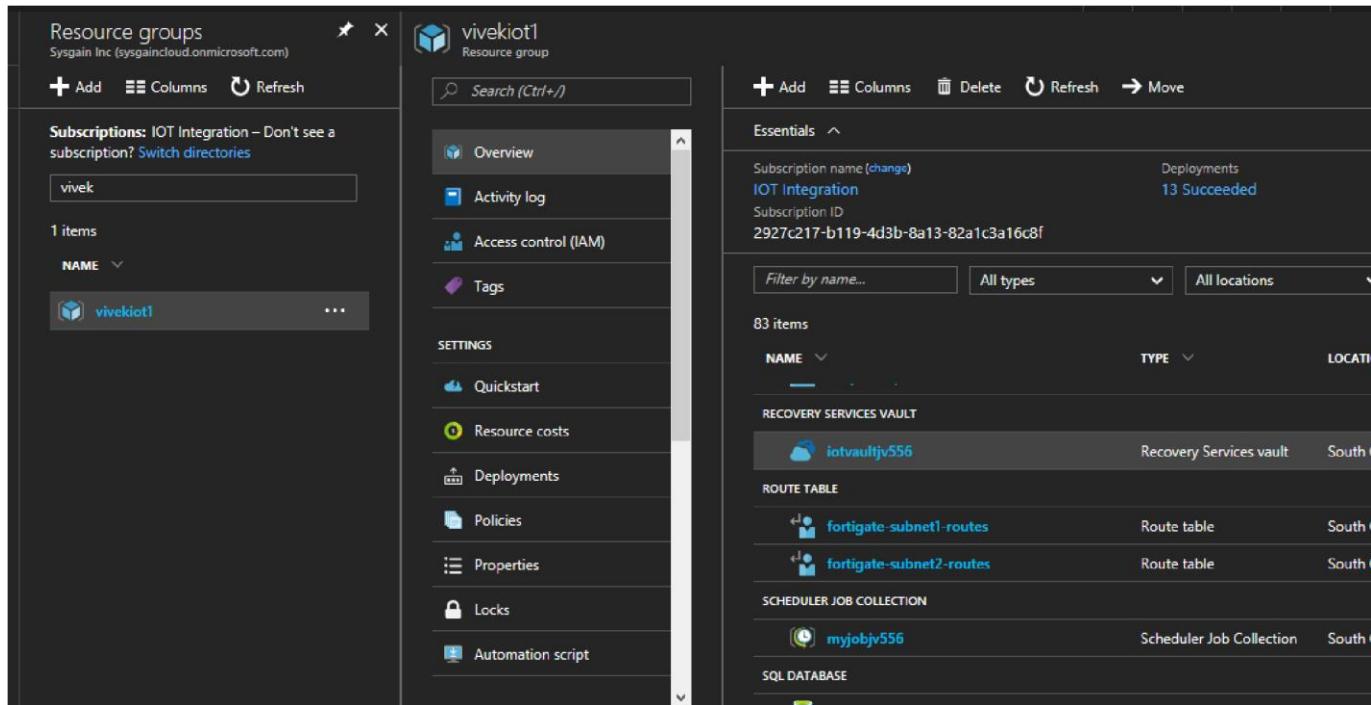
Protect your data by taking snapshots of your data at defined intervals. These snapshots are known as recovery points, and they are stored in recovery services vaults. If or when it is necessary to repair or rebuild a VM, you can restore the VM from any of the saved recovery points. When you restore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



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. On the right, the 'Essentials' blade is open, listing various Azure services and their details.

Category	Name	Type	Location
Subscription name	IOT Integration	Deployments	13 Succeeded
Subscription ID	2927c217-b119-4d3b-8a13-82a1c3a16c8f		
RECOVERY SERVICES VAULT	iotvaultjv556	Recovery Services vault	South
ROUTE TABLE	fortigate-subnet1-routes	Route table	South
	fortigate-subnet2-routes	Route table	South
SCHEDULER JOB COLLECTION	myjobjv556	Scheduler Job Collection	South
SQL DATABASE			

VM's you want to restore.

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

iotvaultjv556
Recovery Services vault

Search (Ctrl+ /)

- [Overview](#)
- [Activity log](#)
- [Access control \(IAM\)](#)
- [Tags](#)
- [Diagnose and solve problems](#)

SETTINGS

- [Properties](#)
- [Locks](#)
- [Automation script](#)

GETTING STARTED

- [Backup](#)
- [Site Recovery](#)

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

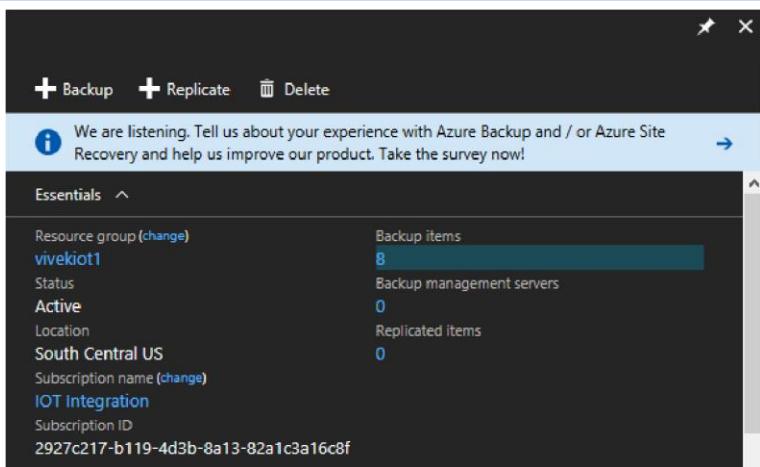
Resource group (change) vivekiot1	Backup items 8
Status Active	Backup management servers 0
Location South Central US	Replicated items 0
Subscription name (change) IOT Integration	
Subscription ID 2927c217-b119-4d3b-8a13-82a1c3a16c8f	

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.



The screenshot shows the 'Backup Items' blade for an Azure Virtual Machine named 'vivekiot1'. The blade has two main sections: a left panel with resource group details and a right panel with a summary of backup items.

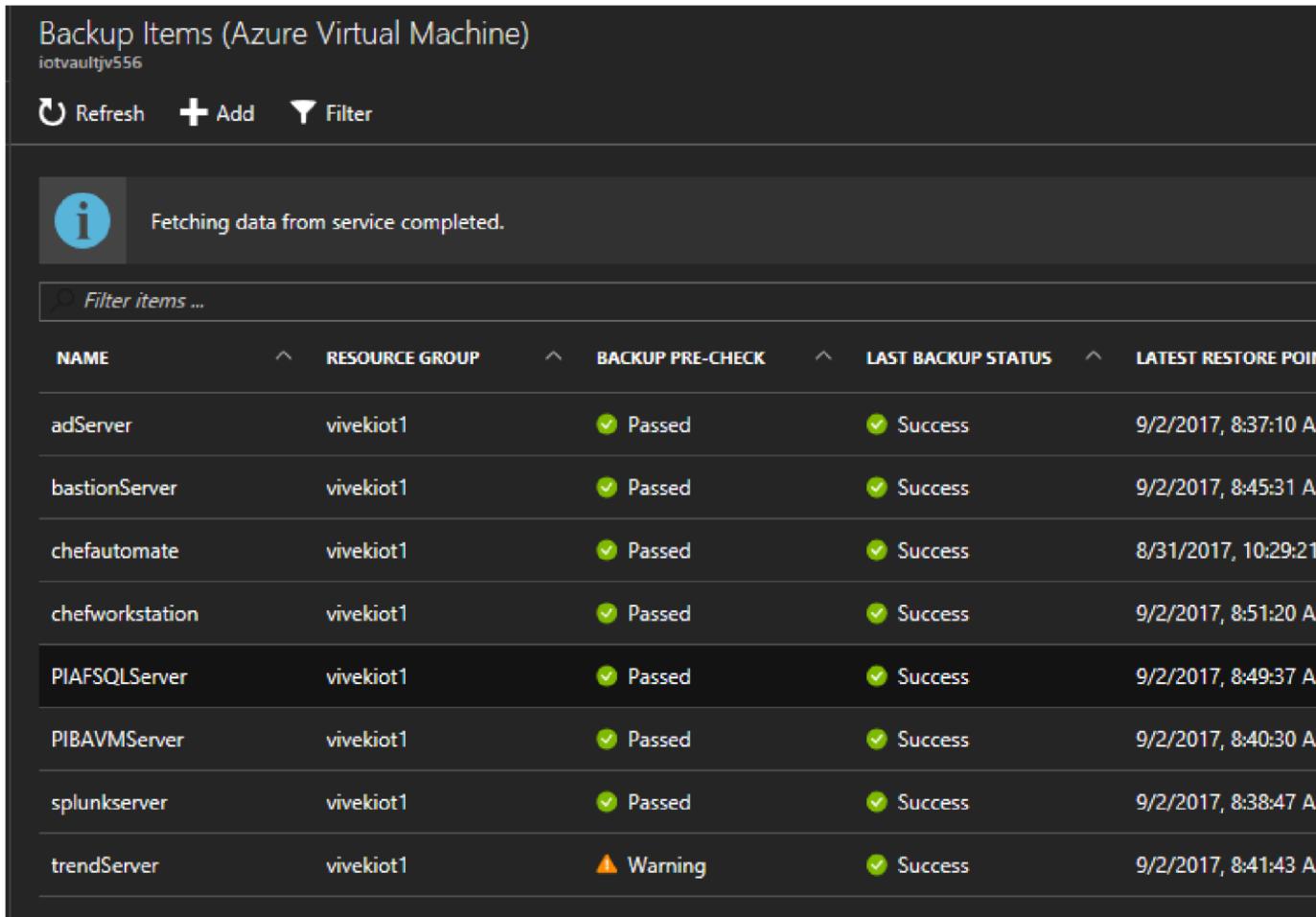
Left Panel (Resource Group Details):

- Resource group ([change](#)): vivekiot1
- Status: Active
- Location: South Central US
- Subscription name ([change](#)): IOT Integration
- Subscription ID: 2927c217-b119-4d3b-8a13-82a1c3a16c8f

Right Panel (Backup Items Summary):

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 the resource group 'iotvaultjv556'. The blade displays a list of VMs with their names, resource groups, backup pre-check status, last backup status, and latest restore point.

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

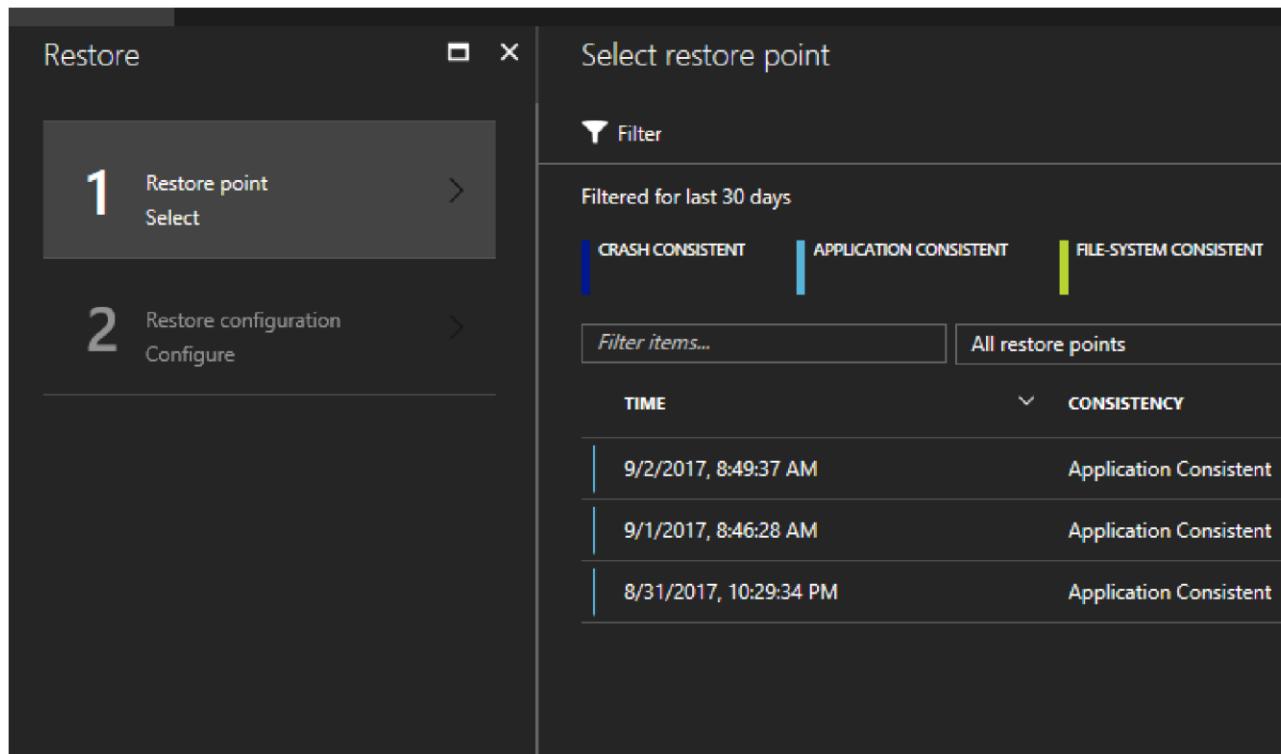
Last 30 days	1
Last 7 days	1

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.

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



Restore point consistency from this list choose:

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

10. Choose a Restore point and click **OK**.

11. The **Restore** blade shows the Restore point is set.

Restore

- 1** Restore point
9/2/2017, 8:49:37 AM
- 2** Restore configuration
Configure

Restore

Select restore point

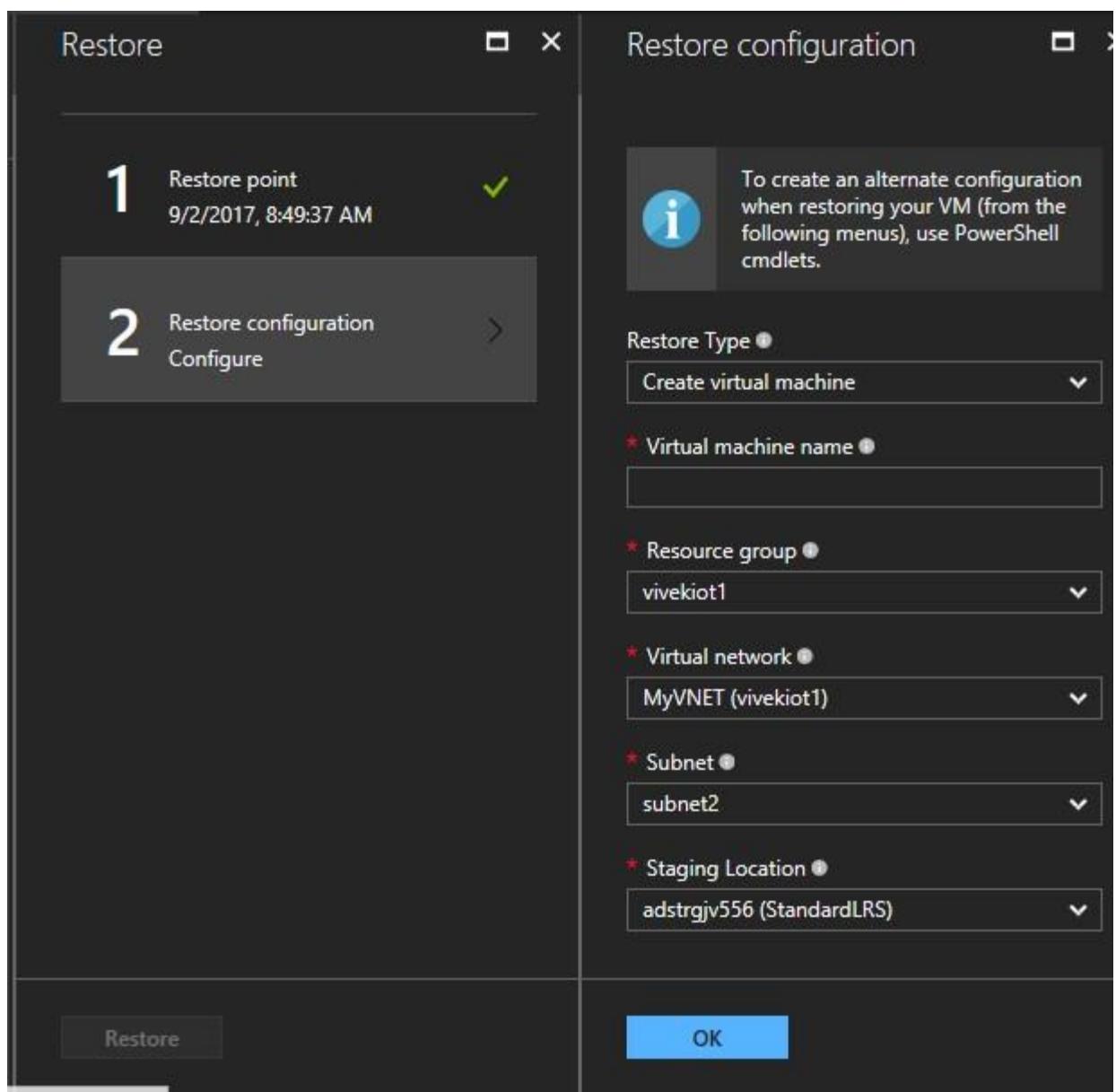
Filter

Filtered for last 30 days

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

OK

12. On the **Restore** blade, **Restore configuration** opens automatically after restore point is set.



14.2. Choosing a VM restore configuration

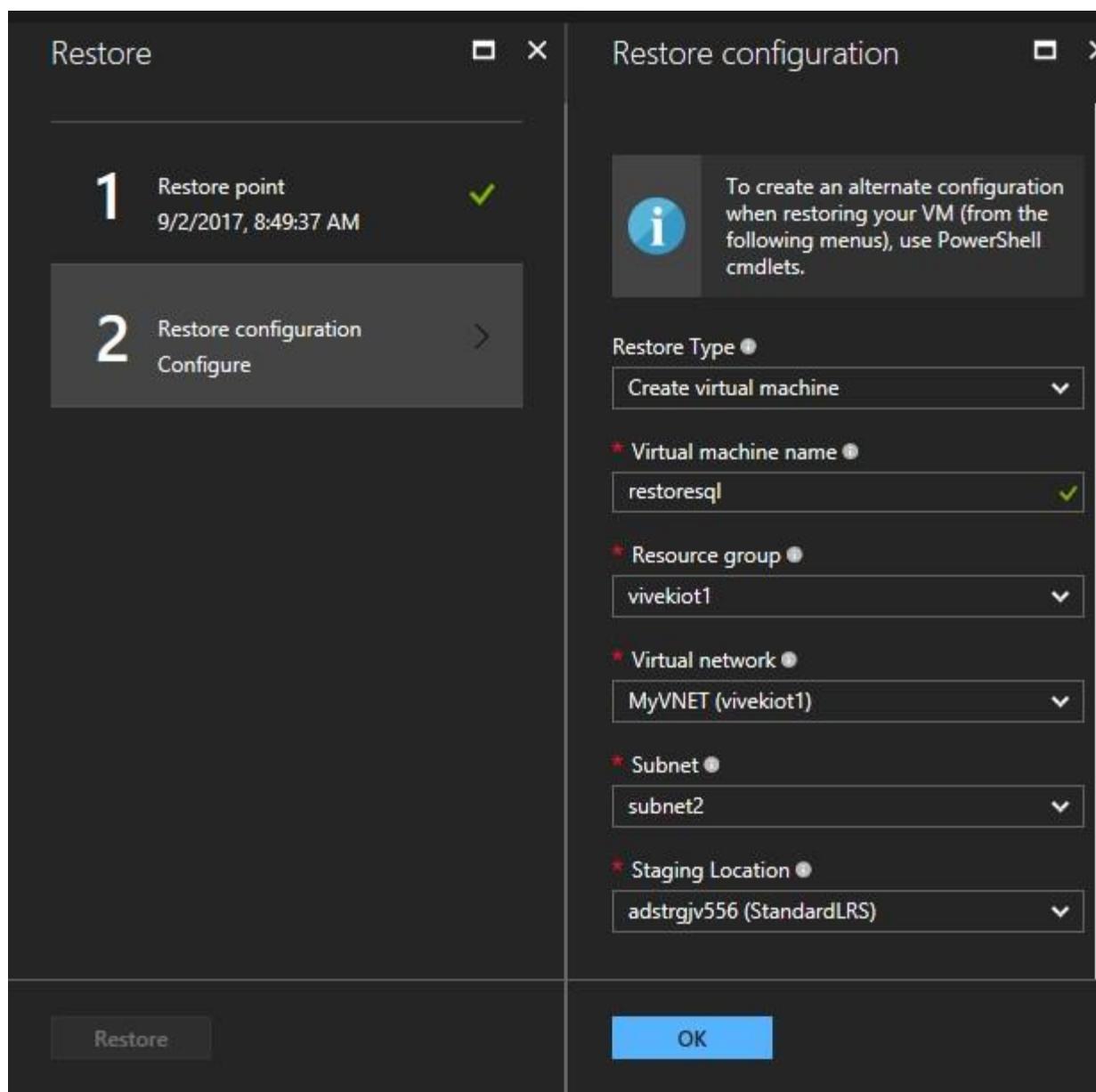
1. Now that you have selected the restore point, choose a configuration for your restore VM.
2. On the **Restore configuration** blade, you have two choices:
 - Restore full virtual machine
 - Restore backed up disks

14.2.1. Create a new VM from restore point

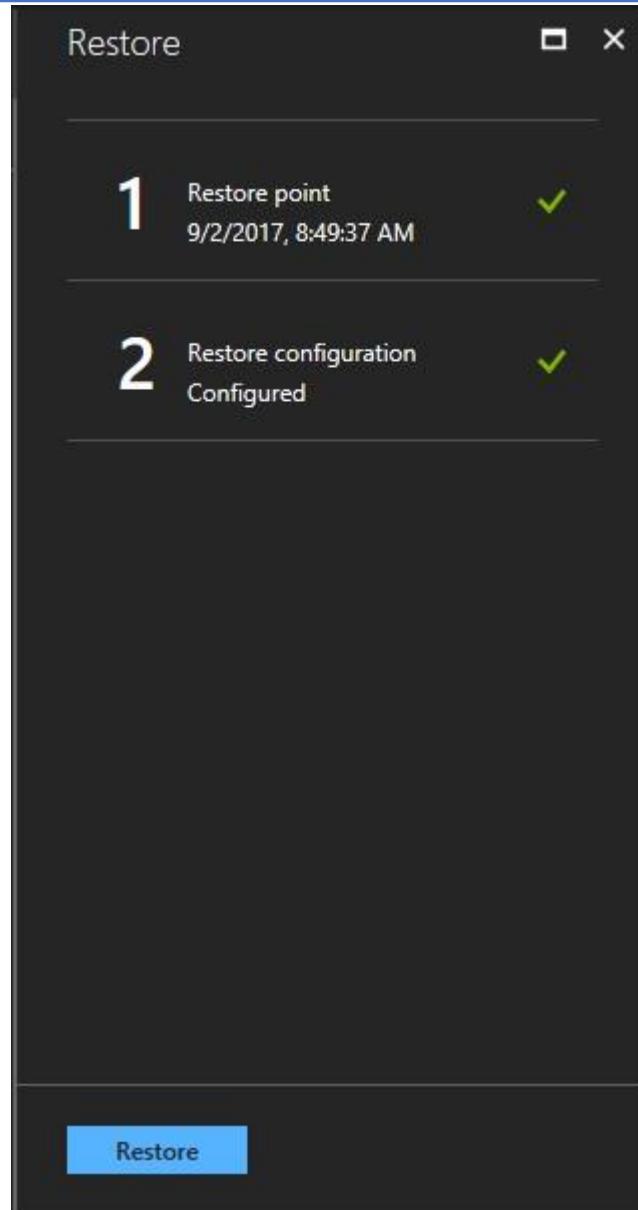
Select Restore Type as Create virtual machine.

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

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

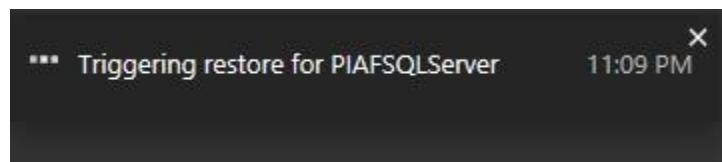


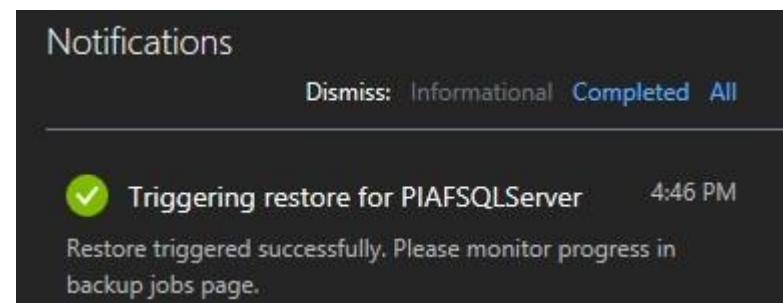
7. On the **Restore configuration** blade, click **OK** to finalize the restore configuration.
8. On the **Restore** blade, click **Restore** to trigger the restore operation.



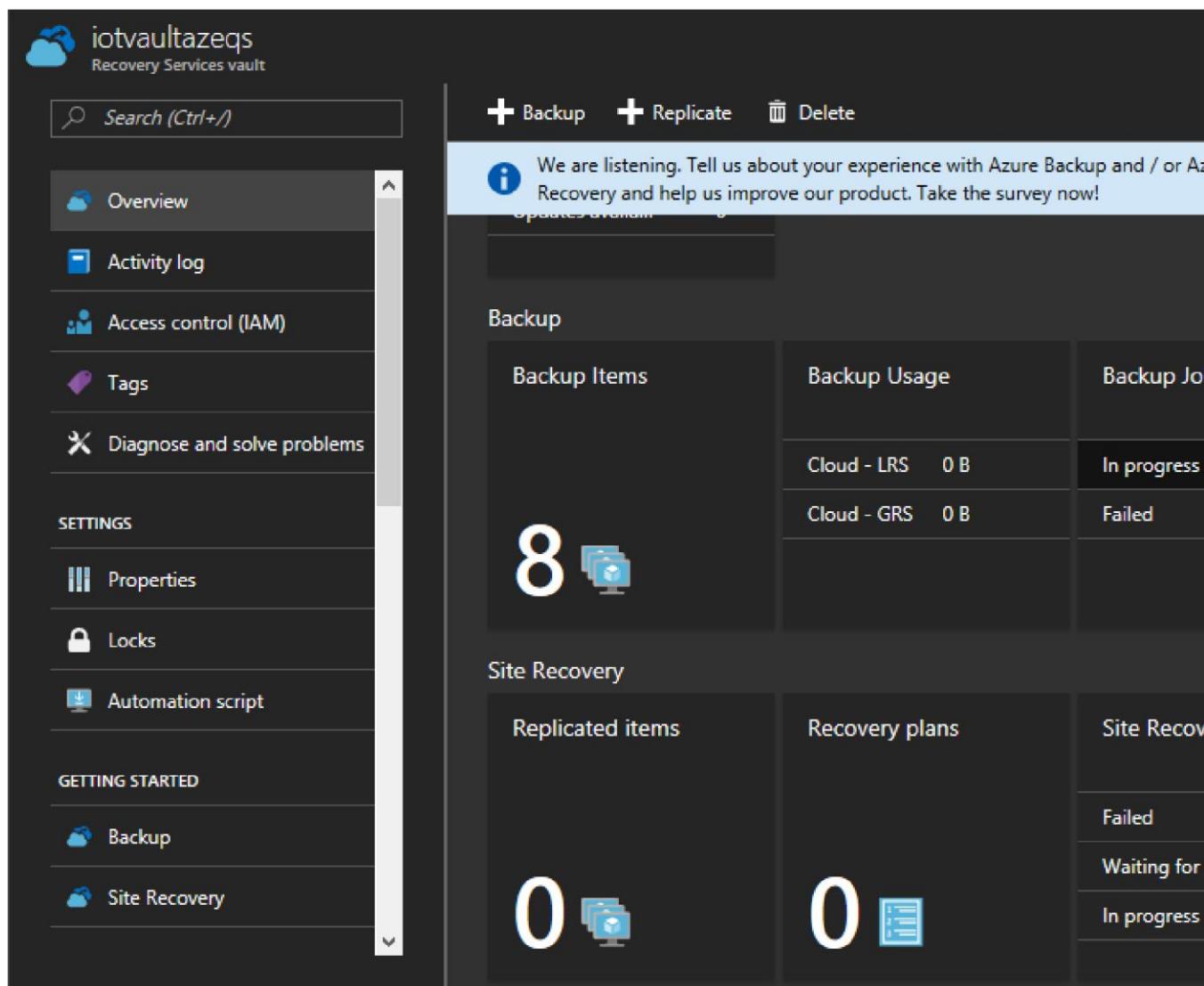
14.3. Track the restore operation

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





2. To view the operation while it is processing, or to view when it completed, open the Backup jobs list.



iotvaultazeqs
Recovery Services vault

Backup **Replicate** **Delete**

We are listening. Tell us about your experience with Azure Backup and / or A...

Backup

Backup Items	Backup Usage	Backup Jobs
Cloud - LRS	0 B	In progress
Cloud - GRS	0 B	Failed

Site Recovery

Replicated items	Recovery plans	Site Recovery Jobs
0	0	Failed
Waiting for	In progress	

SETTINGS

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

GETTING STARTED

- Backup
- Site Recovery



-
3. In the vault dashboard on the **Backup Jobs** tile, click **Azure Virtual Machines** to display the jobs associated with the vault.

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

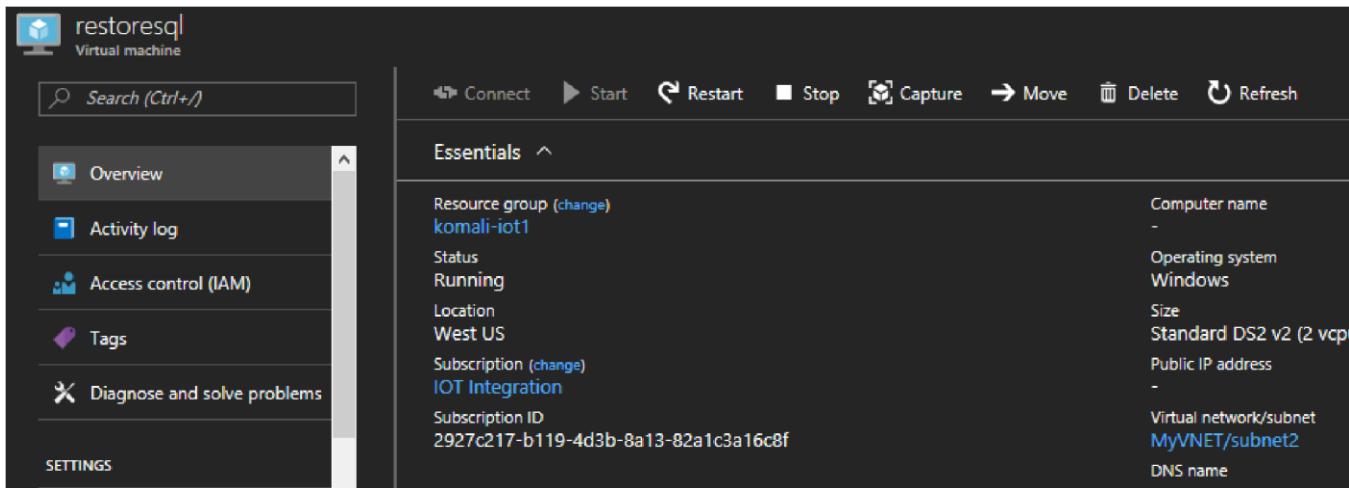
WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION
PIAFSQLServer	Restore	In progress	Azure virtual machine	9/1/2017, 4:45:21 PM	00:02:05

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

NAME	TYPE	LOCATION	... More
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	...

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

Post-Restore steps



restoresql | Virtual machine

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Connect Start Restart Stop Capture Move Delete Refresh

Essentials

Resource group (change) komali-iot1 Computer name -

Status Running Operating system Windows

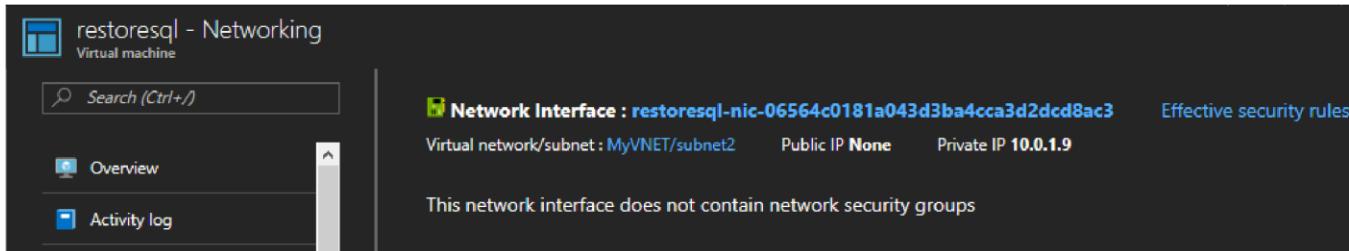
Location West US Size Standard DS2 v2 (2 vcpus)

Subscription (change) IOT Integration Public IP address -

Subscription ID 2927c217-b119-4d3b-8a13-82a1c3a16c8f Virtual network/subnet MyVNET/subnet2

DNS name

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



restoresql - Networking | Virtual machine

Search (Ctrl+ /)

Overview

Activity log

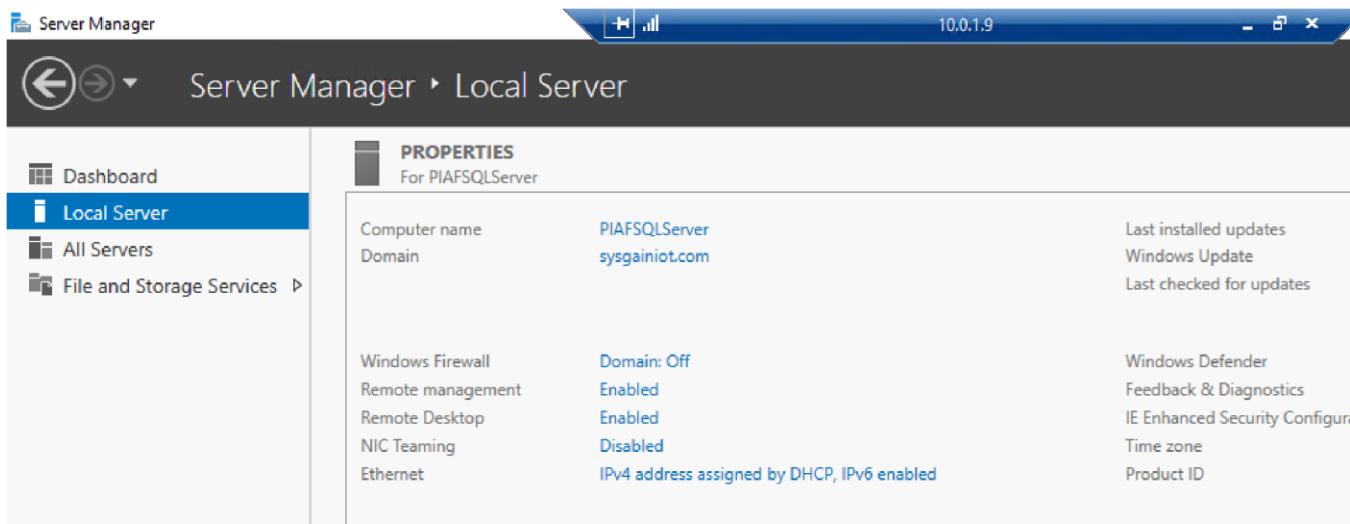
Network Interface : restoresql-nic-06564c0181a043d3ba4cca3d2dcdb8ac3 Effective security rules

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

This network interface does not contain network security groups

conflict when creating restored VM.

2. Login to that VM using its newly created IP.
3. And check whether it has all the restored data or not.

The screenshot shows the "Server Manager" interface. The title bar says "Server Manager" and "10.0.1.9". The left navigation pane shows "Dashboard", "Local Server" (which is selected), "All Servers", and "File and Storage Services". The main pane is titled "PROPERTIES For PIAFSQLServer". It lists the following information:

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

8

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

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

azuredb Execute Debug Generic De

Object Explorer

```
SQLQuery3.sql - sql...redb (sqluser (101)) X SQLQuery2.sql - sql...uredb (sqluser (98)) SQLQuery1.sql - sql...uredb (sqluse
***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [Id]
    ,[AMPS_L1]
    ,[AMPS_L2]
    ,[AMPS_L3]
    ,[AMPS_SYSTEM_AVG]
    ,[Breaker_details]
    ,[Breaker_label]
    ,[Building]
    ,[ClassOccupancyRemaining]
    ,[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 em
2	2	69.3024981644668	70.1256970119966	69.7910198822566	69.7910198822566	New (2013) 4th floor panel - almost em
3	3	108.796504197208	110.088826396877	109.563423955192	109.563423955192	New (2018) 4th floor panel - almost em
4	4	67.8138422158681	68.6193582973547	68.2918702172629	68.2918702172629	New (2013) 3rd floor panel - almost em
5	5	71.1518101662343	71.9969757761305	71.6533679086951	71.6533679086951	New (2013) 4th floor panel - almost em
6	6	110.19703573853	111.5059939323	110.973828013269	110.973828013269	New (2018) 4th floor panel - almost em
7	7	70.3289157499257	71.1643067376498	70.8246728098071	70.0591480335381	New (2013) 3rd floor panel - almost em
8	8	67.0645549558174	67.8611707461849	67.5373011404077	67.5373011404077	New (2013) 4th floor panel - almost em
9	9	117.80439541763	119.203716439385	118.634812893722	118.634812893722	New (2018) 4th floor panel - almost em
10	10	56.4886592177897	57.159650890503	56.8868546301863	56.8868546301863	New (2013) 3rd floor panel - almost em

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.

