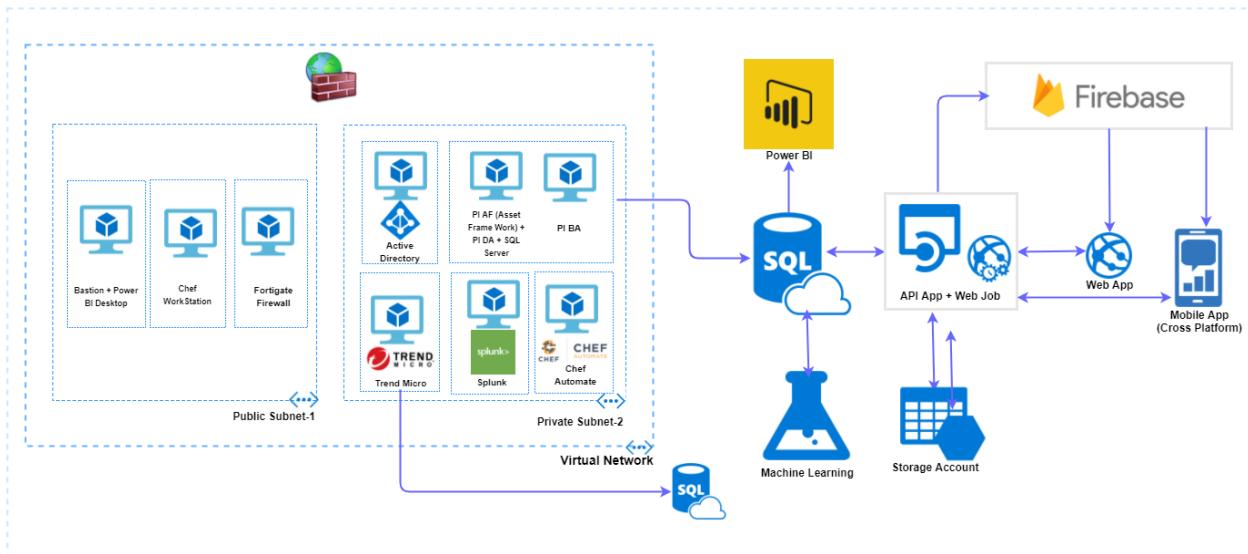


Contents

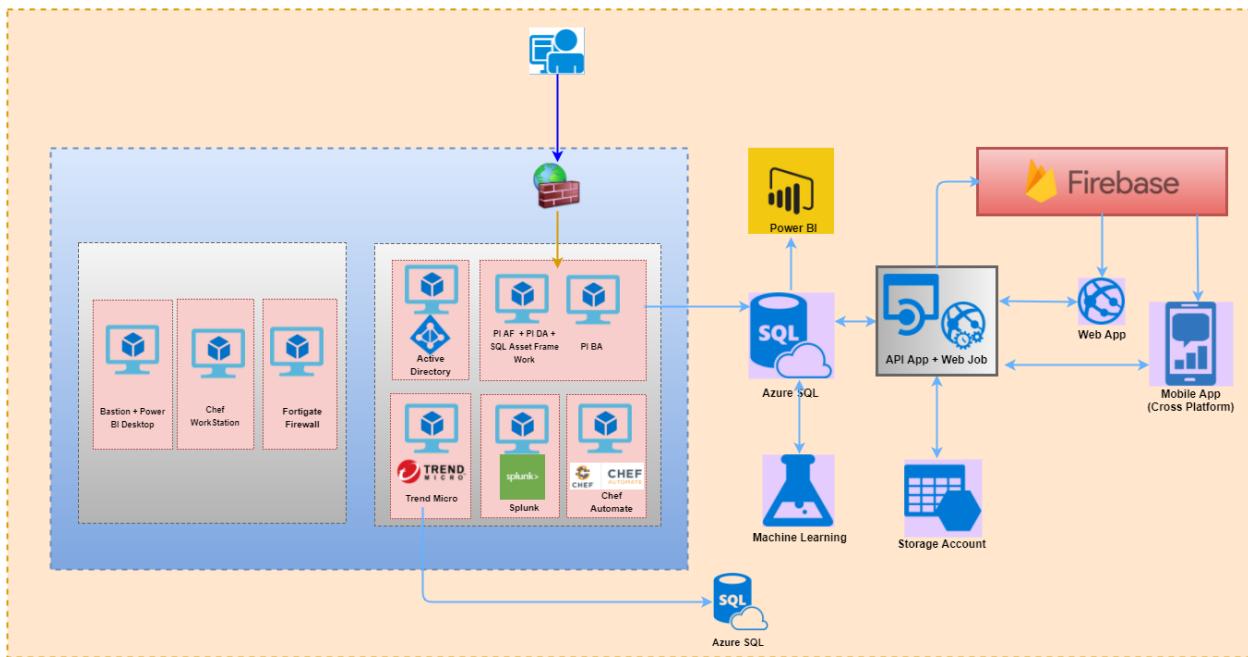
1.	Architecture	3
1.1.	Data Flow Architecture Diagram.....	3
2.	High Level Deployment Process to be Followed.....	4
3.	Deployment Costs	5
4.	Prerequisites.....	7
4.1.	Azure B2C Tenant Creation and Configuration	7
4.2.	Power BI Configuration.....	27
4.3.	Dynatrace Account Creation (If You Don't Have An Existing Account).....	33
5.	Input Parameters	37
6.	Azure Resource Manager Template Deployment	39
6.1.	OutPut Parameters	45
7.	Security And Monitoring Components.....	48
7.1.	Dynatrace.....	48
7.1.1.	Installing Dynatraceoneagent To Web Application (PaaS Environment)	60
7.2.	Chef Automate.....	71
7.3.	Splunk.....	76
7.4.	TrendMicro	78
8.	Create User for PI Business Analytics (PIBA) Interface	94
8.1.	Create PIBA User in PIAF Server	104
8.2.	Enable TCP and Named Pipe in SQL Server Configuration Management.....	111
9.	Components of PI Server.....	113
9.1.	PI Asset FrameWork (AF)	113
9.1.1.	Installation of PIAF Server	114
9.2.	PI Data Archive (PIDA).....	116
9.2.1.	Installation of Data Archive (PIDA).....	117
9.3.	PI Web API Utility	126
9.4.	Creation of Database in PI System Explorer	132
9.5.	System Configuration in PI System Explorer	135

9.6. Import .XML Files into AF Server	139
9.7. Update Security in PI System Management Tools	146
9.8. Prepare Data Server For Module Database(Mdb) To Asset Framework(AF)	158
9.9. Update PI Points in PI System Explorer	163
9.10. Install And Run The Piweb Simulator Setup	168
10. Installation of PI BA Integrator.....	173
10.1. Configuring PI Business Analytics.....	180
11. Configuring And Accessing The Webapp.....	219
12. Machine Learning Experiment	225
13. Firebase Configuration.....	237

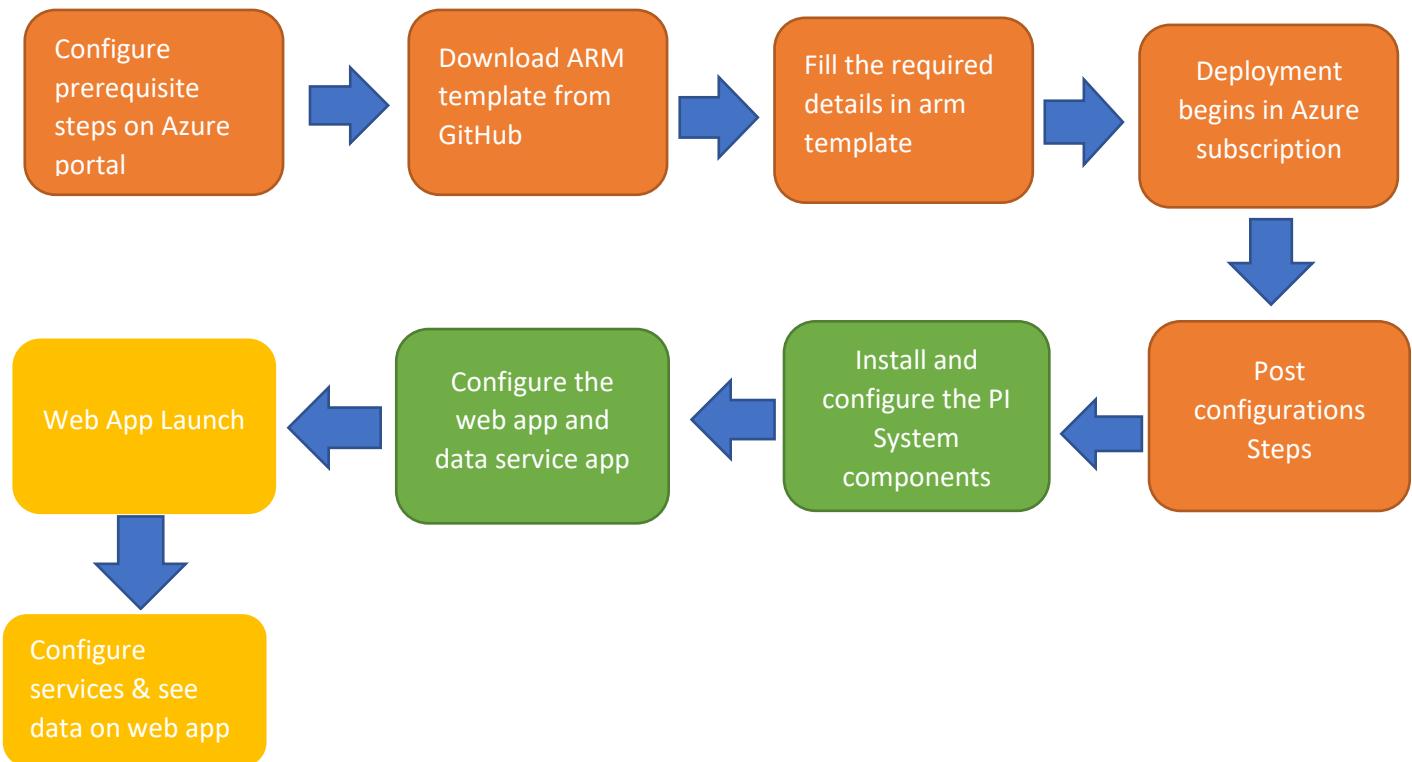
1. Architecture

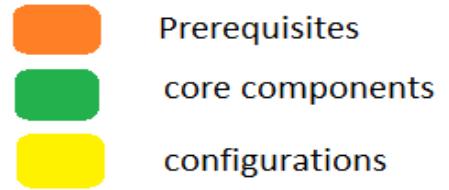


1.1. Data Flow Architecture Diagram



2. High Level Deployment Process to be Followed





3. Deployment Costs

VM Name	VMSize	OS	Software Cost	Azure Cost
Bastion Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2012 R2	PAYG	\$ 0.21/Hour
Chef Automate Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	\$ 0.14/Hour
Active Directory Server	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2016	PAYG	\$ 0.21/Hour
Chef workstation	Standard_DS2_v2 (2 cores, 7 GB memory)	Windows 2012 R2	PAYG	\$ 0.21/Hour
PIAFSQL Server	Standard_DS2_v2 (2 core, 7 GB memory)	Windows 2016 + SQL 2016SP1	BYOL	\$0.61/Hour
PIBAVM Server	Standard DS4 v2 (8 cores, 28 GB memory)	Windows 2012 R2	BYOL	\$ 0.84/Hour
Splunk Server	Standard DS2 v2 (2 cores, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	\$ 0.14/Hour
Trend Micro	Standard DS2 v2 (2 cores, 7 GB memory)	CentOS 7	BYOL	\$ 0.14/Hour
Web App	S1 Standard (1 instance)			\$ 0.1/Hour
API App	S1 Standard (1 instance)			\$ 0.1/Hour
FortiGate Firewall	Standard D2 v2 (2 core, 7 GB memory)	Ubuntu 14.04 LTS	BYOL	\$ 0.14/Hour
Machine Learning	S1 Standard			\$9.99 per seat/month, \$1 per studio experimentation/hour

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

4. Prerequisites

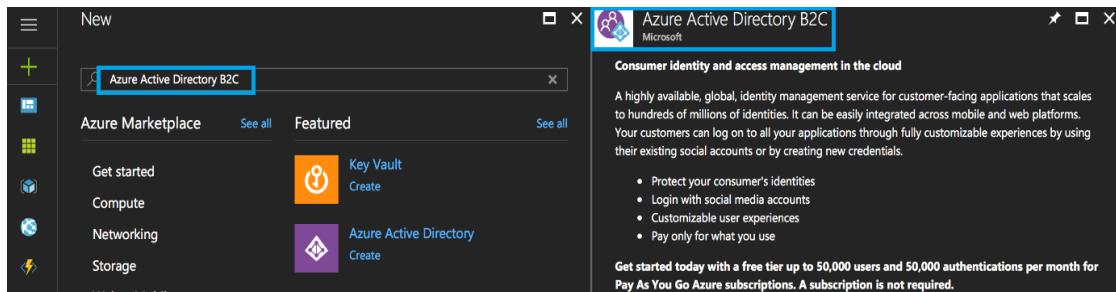
1. The Azure AD B2C Tenant should be created and register your web application.
2. Create an account in Power BI.
3. Dynatrace account creation in SAAS.

4.1. Azure B2C Tenant Creation and Configuration

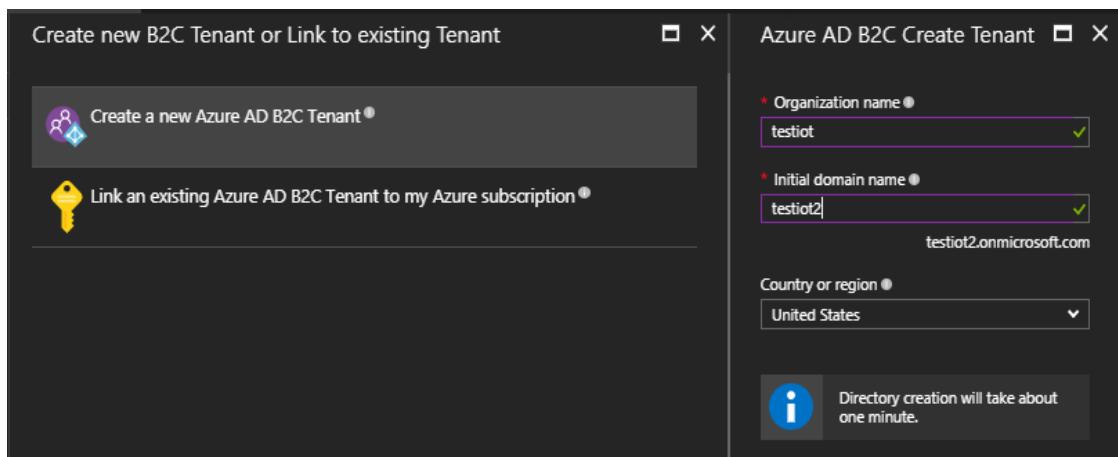
Creating Azure AD B2C tenant is a one-time activity, if you have a B2C Tenant already created by your admin then you should be added into that tenant as Global Administrator to register your app to get the B2C tenant id, application id and sign-in/sign-up policies.

Follow Below steps to create Azure AD B2C Tenant:

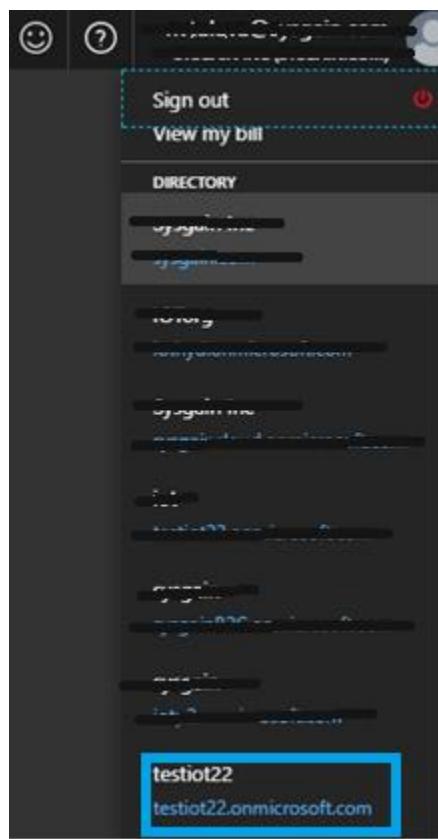
1. Create a new B2C tenant in **Azure Active Directory B2C**. You'll be shown a page with the information on Azure Active Directory B2C. Click **Create** at the bottom to start configuring your new Azure Active Directory B2C tenant.



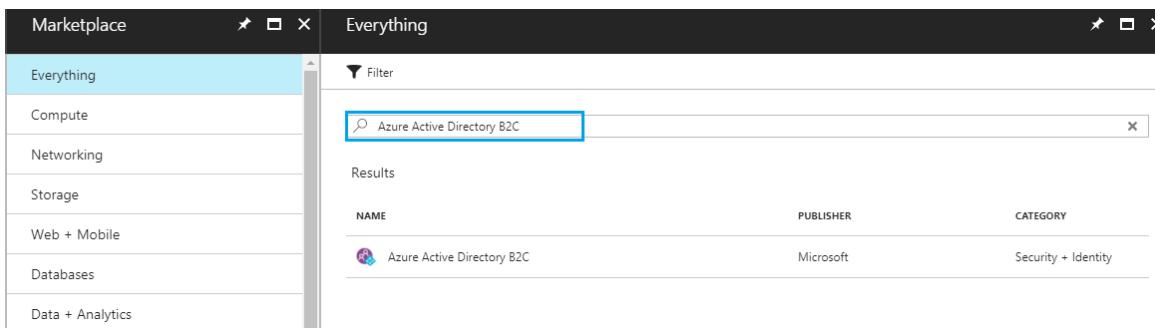
2. Choose the **Organization name**, **Initial Domain name** and **Country or Region** for your Tenant.



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



- Go to the Marketplace and search for **Azure Active Directory B2C**, then click on it.



5. Click on **Link an existing Azure AD B2C Tenant** and provide the required details. Once done, click on **Create**.

This image shows two windows side-by-side. The window on the left is titled 'Create new B2C Tenant or Link to existing Tenant'. It has two main options: 'Create a new Azure AD B2C Tenant' (with a purple icon) and 'Link an existing Azure AD B2C Tenant to my Azure subscription' (with a yellow key icon). The second option is highlighted with a blue box. The window on the right is titled 'Azure AD B2C Resource'. It contains several configuration fields:

- * Azure AD B2C Tenant: testiot22.onmicrosoft.com
- Azure AD B2C Resource name: testiot22.onmicrosoft.com
- * Subscription: IOT Integration
- Resource group:
 - Create new: iotRG (selected)
 - Use existing: (unchecked)
- Resource group location: East Asia

At the bottom of the right window is a 'Create' button.

6. Click on the **Tenant name** you created, navigate to **Azure Active Directory B2C** and click on **Sign-up policies**. Then click on **Add** to add policy.

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

Search (Ctrl+F)

+ Add Upload Policy

Overview

MANAGE

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

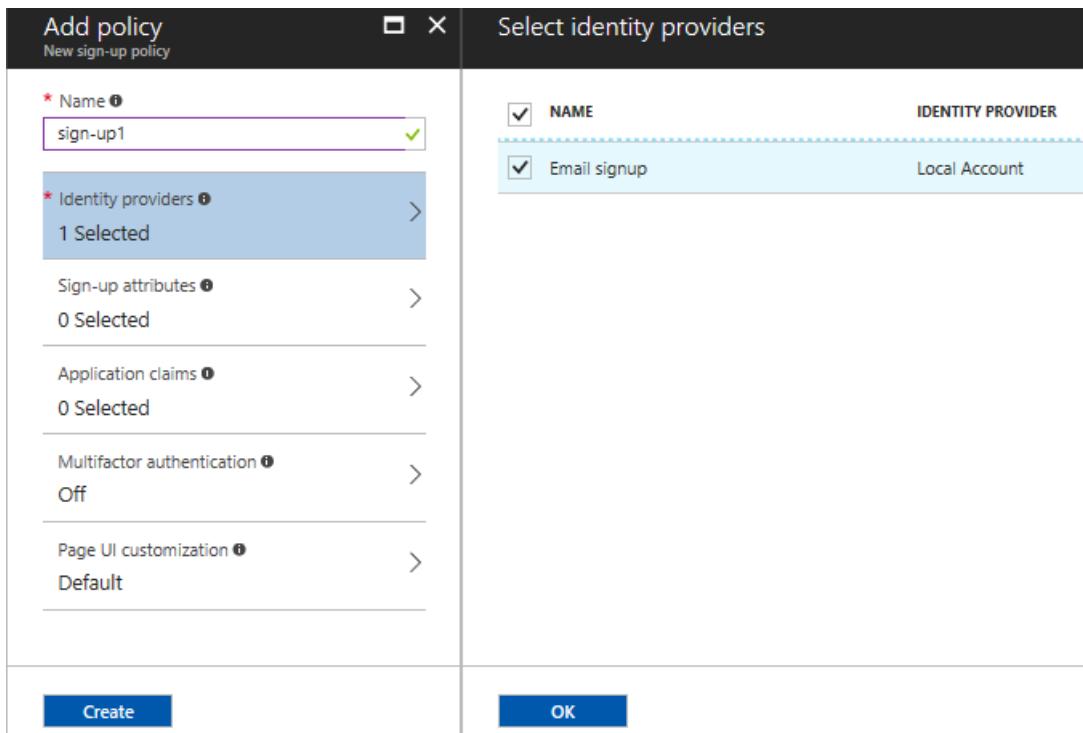
POLICIES

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

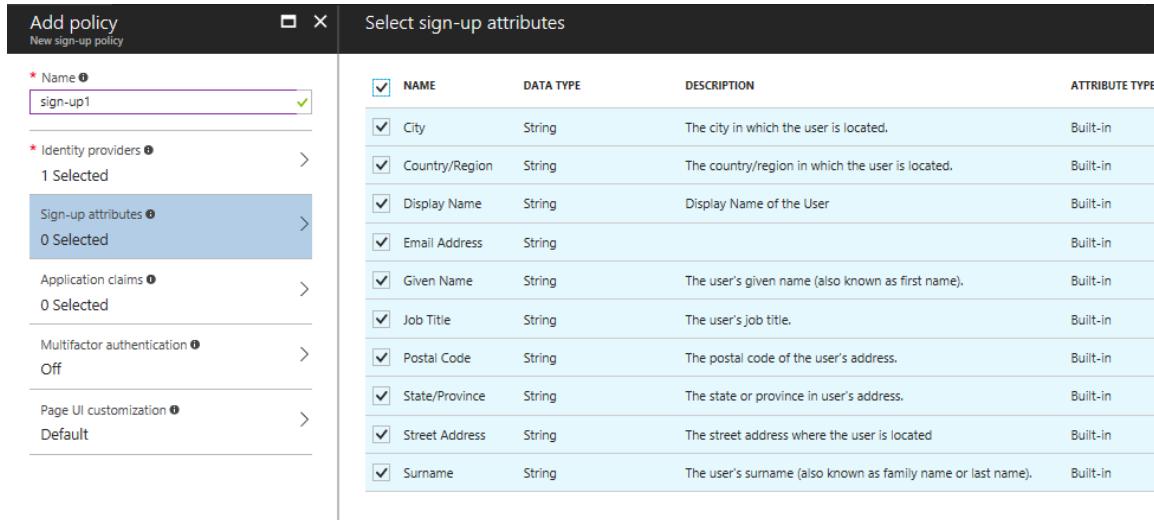
B2C_1_sign-up1
Default template

Add

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



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



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

Add policy □ X

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

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

The screenshot shows the Azure AD B2C - Sign-up policies interface. The left sidebar has a 'Search (Ctrl+/' input field and a navigation menu with sections 'MANAGE' and 'POLICIES'. Under 'POLICIES', the 'Sign-up or sign-in policies' section is expanded, showing options for 'Sign-up policies', 'Sign-in policies', and 'All policies'. The 'Sign-up policies' option is highlighted with a blue background. The main content area shows a search bar and a list of policies: 'B2C_1_sign-up1' (Default template). At the top right, there are 'Add' and 'Upload Policy' buttons.

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

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

The screenshot shows the Azure AD B2C Sign-in policies interface. On the left, there's a sidebar with 'MANAGE' and 'POLICIES' sections. Under 'POLICIES', 'Sign-in policies' is highlighted with a blue background. Other options like 'Sign-up or sign-in policies', 'Profile editing policies', 'Password reset policies', and 'Sign-up policies' are also listed. At the top right, there are 'Add' and 'Upload Policy' buttons.

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

The screenshot shows two overlapping windows. The left window is titled 'Add policy' and has a sub-header 'New sign-in policy'. It contains fields for 'Name' (set to 'sign-in1'), 'Identity providers' (set to '0 Selected'), 'Application claims' (set to '0 Selected'), 'Multifactor authentication' (set to 'Off'), and 'Page UI customization' (set to 'Default'). At the bottom are 'Create' and 'OK' buttons. The right window is titled 'Select identity providers' and lists a single provider: 'Local Account SignIn' under 'IDENTITY PROVIDER'. Both windows have close ('X') buttons at the top right.

13. Select all Application claim

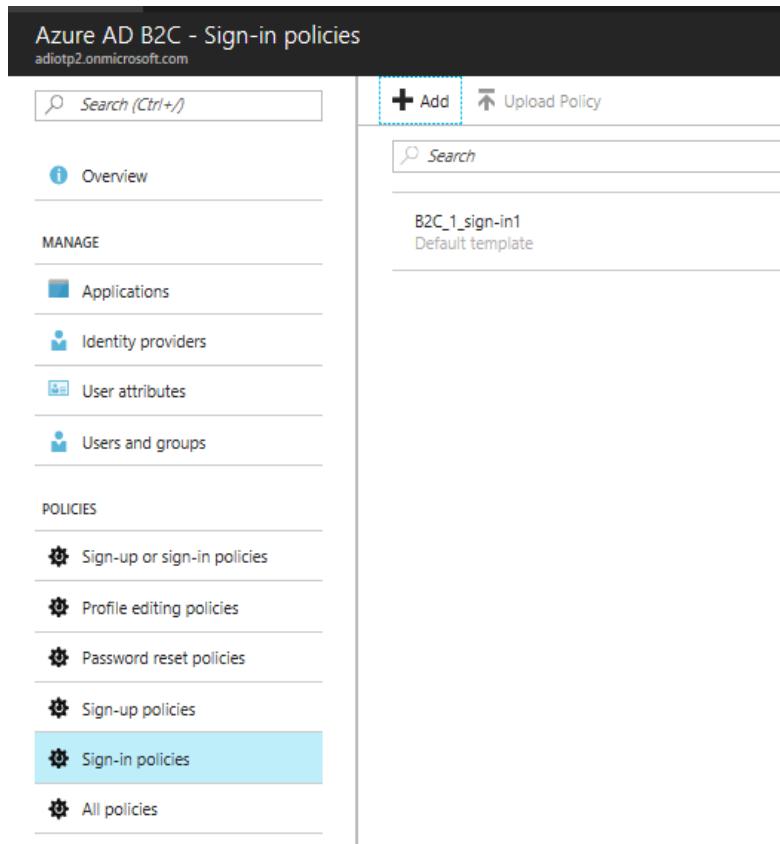
The screenshot shows the 'Select application claims' dialog box. It lists 12 claims under the 'NAME' column, each with a checked checkbox. The columns are labeled: NAME, CLAIM TYPE, DATA TYPE, DESCRIPTION, and ATTRIBUTE TYPE. The claims include: City, Country/Region, DisplayName, Email Addresses, Given Name, Identity Provider, Job Title, Postal Code, State/Province, Street Address, Surname, and User's Object ID. At the bottom of the dialog are 'Create' and 'OK' buttons.

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
DisplayName	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

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

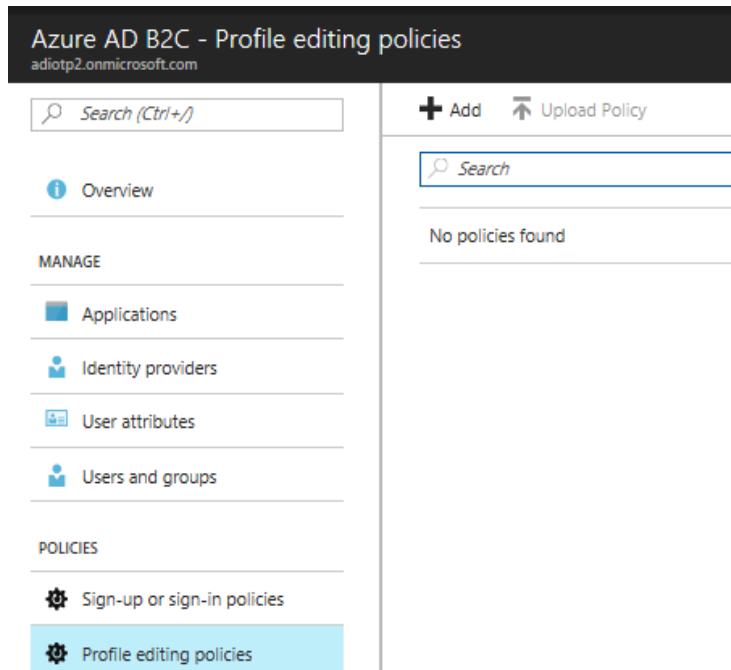
The screenshot shows the 'Add policy' dialog box. It has sections for 'Name' (sign-in1), 'Identity providers' (1 Selected), 'Application claims' (12 Selected), 'Multifactor authentication' (Off), and 'Page UI customization' (Default). The 'Application claims' section is highlighted with a blue dashed border. At the bottom are 'Create' and 'OK' buttons.

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



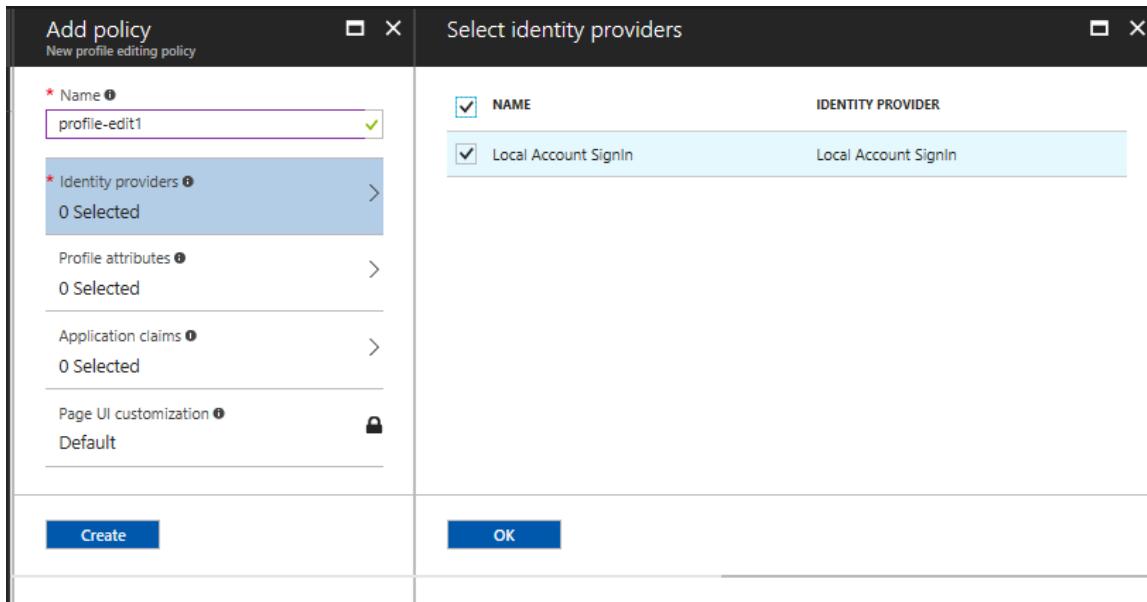
The screenshot shows the Azure AD B2C - Sign-in policies interface. The left sidebar has a search bar at the top, followed by sections for Overview, MANAGE (Applications, Identity providers, User attributes, Users and groups), and POLICIES (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Sign-in policies' option is highlighted with a blue background. The main right area shows a search bar and a list item: 'B2C_1_sign-in1' (Default template).

16. Click on **Profile editing policies**

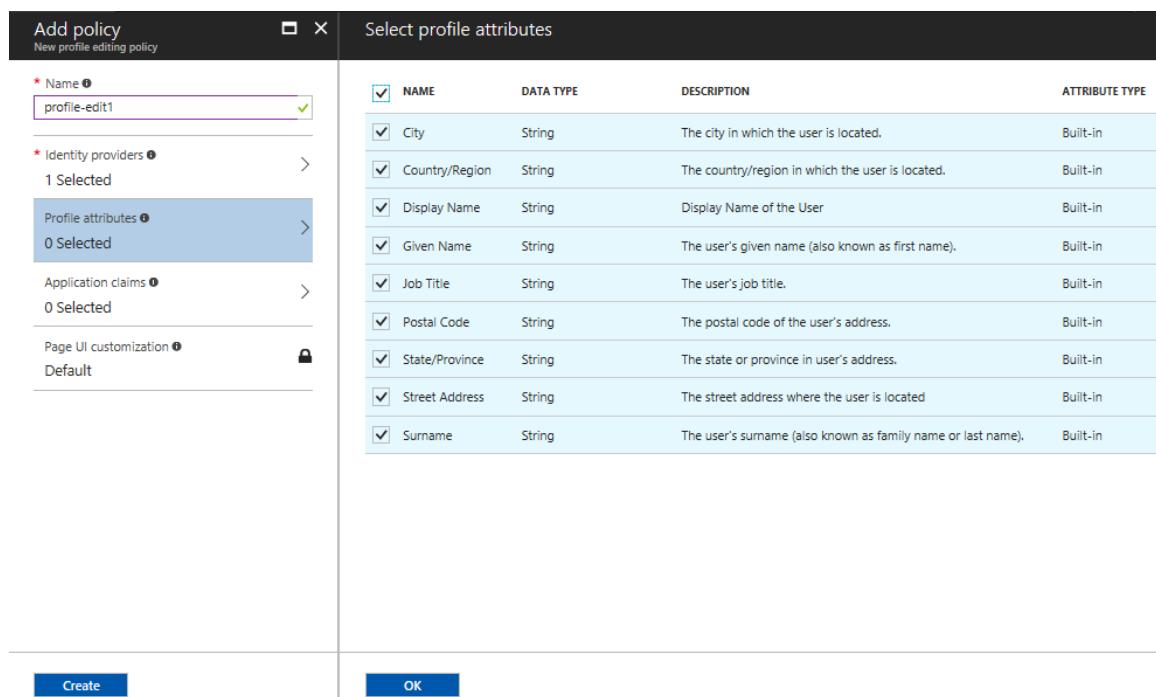


The screenshot shows the Azure AD B2C - Profile editing policies interface. The left sidebar has a search bar at the top, followed by sections for Overview, MANAGE (Applications, Identity providers, User attributes, Users and groups), and POLICIES (Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies, Sign-in policies, All policies). The 'Profile editing policies' option is highlighted with a blue background. The main right area shows a search bar and a message: 'No policies found'.

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



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



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

Add policy

New profile editing policy

* Name

* Identity providers

Profile attributes

Application claims

Page UI customization

Create

Select application claims

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

OK

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

Add policy

New profile editing policy

* Name

* Identity providers

Profile attributes

Application claims

Page UI customization

Create

21. 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 'MANAGE' section with links for Applications, Identity providers, User attributes, and Users and groups. The 'POLICIES' section contains four items: Sign-up or sign-in policies, Profile editing policies (which is highlighted with a blue background), Password reset policies, and Sign-up policies. The main content area has a search bar and two buttons: '+ Add' and 'Upload Policy'. Below these buttons, there is a list item: 'B2C_1_profile-edit1 Default template'.

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

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

Search (Ctrl+)

Overview

MANAGE

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

POLICIES

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

+ Add Upload Policy

No policies found

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

Add policy X

New password reset policy

* Name i
password-change1 ✓

* Identity providers i >
0 Selected

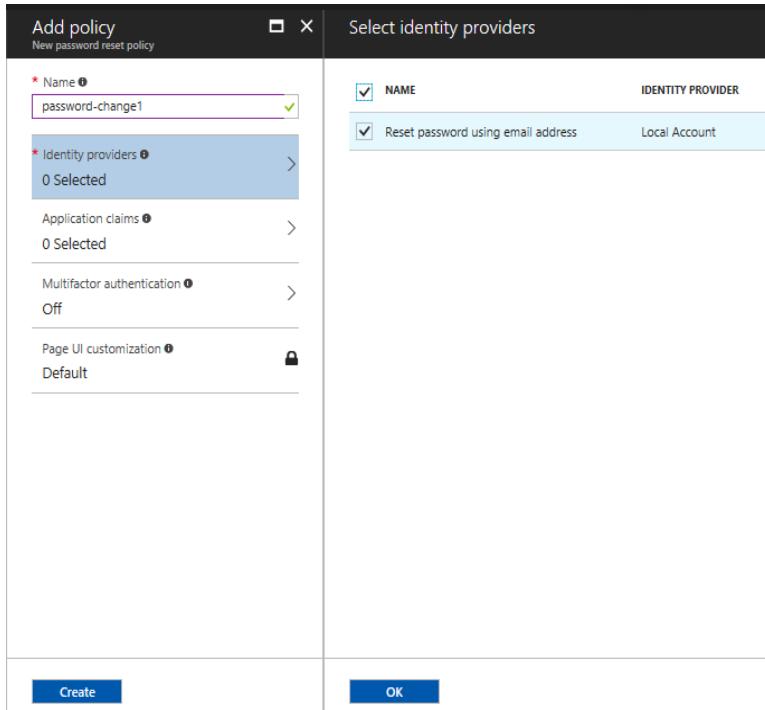
Application claims i >
0 Selected

Multifactor authentication i >
Off

Page UI customization i 🔒
Default

Create

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



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

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

26. Click on **Create**.

Add policy X

New password reset policy

* Name !
password-change1 ✓

* Identity providers ! >
1 Selected

Application claims ! >
11 Selected

Multifactor authentication ! >
Off

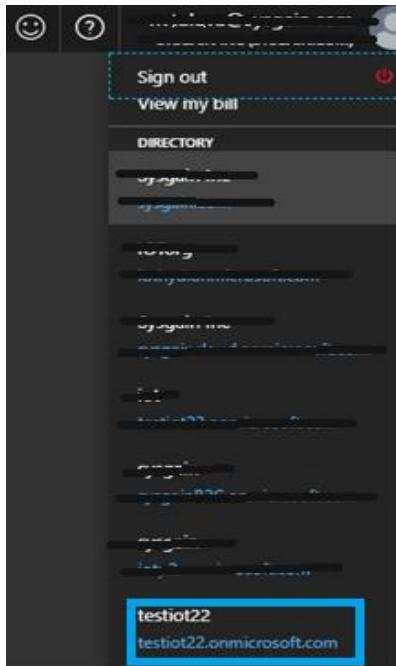
Page UI customization ! >
Default

Create

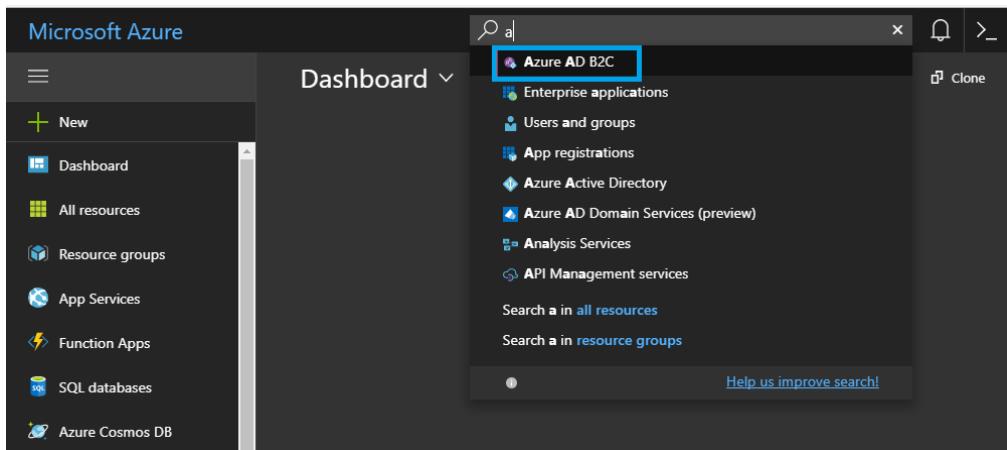
27. Once the deployment is completed, the below screen will appear.

The screenshot shows the Azure AD B2C - Password reset policies interface. At the top left, it says "Azure AD B2C - Password reset policies" and "adiotp2.onmicrosoft.com". On the left, there's a sidebar with a search bar and a "Manage" section containing links for Applications, Identity providers, User attributes, and Users and groups. Below that is a "Policies" section with links for Sign-up or sign-in policies, Profile editing policies, Password reset policies (which is highlighted with a blue background), Sign-up policies, Sign-in policies, and All policies. At the top right, there are "Add" and "Upload Policy" buttons, and a search bar. In the main area, there's a list showing one policy: "B2C_1_password-change1" (Default template).

28. The tenant is now created and will appear in the Active Directory extension.



29. After creating the B2C Tenant, click on Azure B2C settings. This will open the overview page.



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

New application

Name ✓

Web App / Web API
Include web app / web API
 Yes No

Native client
Include native client
 Yes No

Create

Microsoft Azure | Azure AD B2C - Applications

testiot22.onmicrosoft.com

+ Add

NAME	APPLICATION ID
contoso	06696b08-2cfa-4315-8fe
webiot1	aa11ca5c-5fb0-4818-bb6
iothydapp	4e0f3368-0160-46d7-865

31. 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:

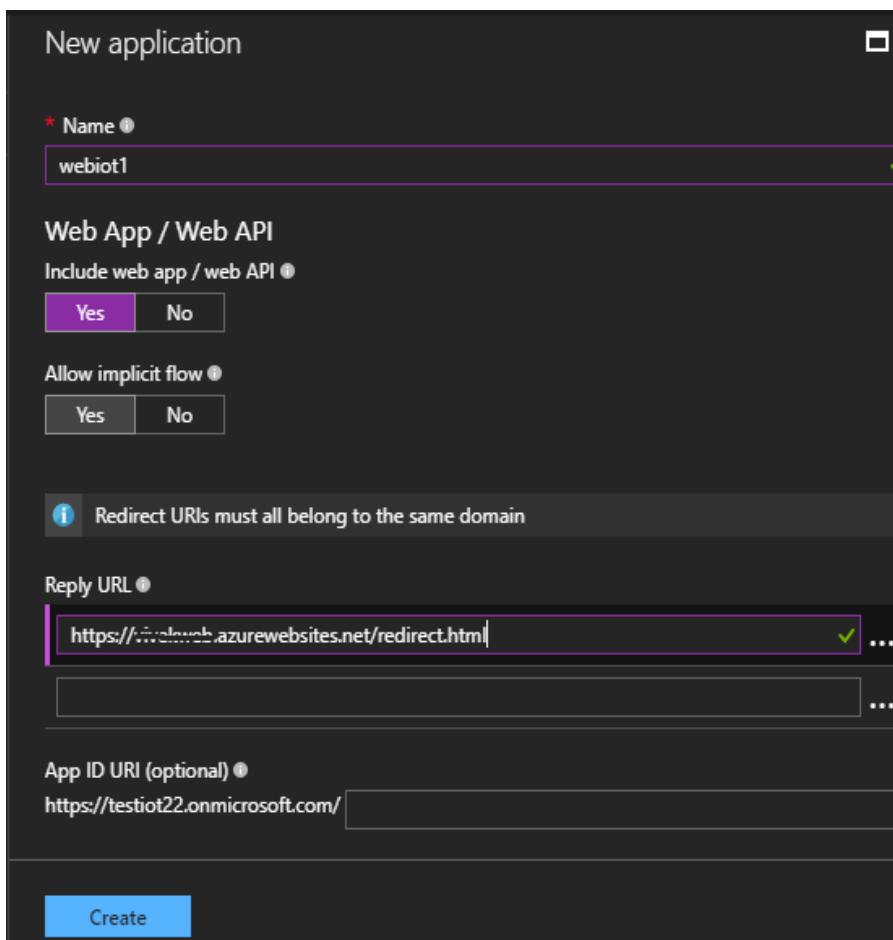
`https://<name of the web app>.azurewebsites.net/redirect.html`

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.



32. 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	
<input type="button" value="Search (Ctrl+I)"/> Add	
NAME	APPLICATION ID
contoso	06696b08-2cfa-4315-81e0-000000000000
webiot1	aa11ca5c-5fb0-4818-bb2d-000000000000
iothydapp	4e0f3368-0160-46d7-8a20-000000000000
demoapp	991b1d9c-5504-4a8e-a200-000000000000

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

The screenshot shows the 'webiot1 - Keys' page. On the left, there's a sidebar with 'GENERAL' and three tabs: 'Properties' (selected), 'Keys' (highlighted with a blue box), and 'APPLY CHANGES / PREVIEW'. On the right, there's a 'Save' button, a 'Discard' button, and a 'Generate key' button (also highlighted with a blue box). Below these buttons, there's a section for 'App key' with a placeholder text '26X*****'.

34. **Copy** the secret key.

The screenshot shows the same 'webiot1 - Keys' page as before, but now it has a second 'App key' entry below the first one. The first key is '26X*****' and the second is '%\$88MxGK%"\$vr6Ofz'. The 'Save' button is highlighted with a blue box.

4.2. 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:

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

Server-side Web app

Redirect URL:

A URL within your web application that will be redirected to when user login completes in order for your app to receive an authorization code for that user.

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

Home Page URL:

The URL for the home page of your application.

https://webapptest.azurewebsites.net

e. Select check boxes for required API's (select all check boxes for best practice).

- Read all datasets
- Read and write all data sets
- Read all dashboards
- Read all reports
- Read and Write all reports
- Read all Groups
- Create content

f. Click on Register App.

Step 3 Choose APIs to access

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

Dataset APIs

- Read All Datasets
- Read and Write All Datasets

Report and Dashboard APIs

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

Other APIs

- Read All Groups
- Create Content

Step 4 Register your app

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

[Register App](#)

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



Power BI for Developers

Step 4 Register your app

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

[Register App](#)

Client ID:

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

Client Secret:

oA6639cMkKuDrvfZQZsQ6/BMd8imml2xDkrbnvoqw+c=

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

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.

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

- Enable the following access under delegated permissions in **Windows Azure Active Directory**.

- Access the directory as the signed in users
- Read directory data
- Read and write all groups

- Read all user's basic profiles
 - Sign in and read user profile
- After that click on **Save**.

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	
<input type="button"/> Save <input type="button"/> Delete	
⚠ 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.	
Read all hidden memberships	<input checked="" type="checkbox"/> Yes
Manage apps that this app creates or owns	<input checked="" type="checkbox"/> Yes
Read and write all applications	<input checked="" type="checkbox"/> Yes
Read and write domains	<input checked="" type="checkbox"/> Yes
<input type="checkbox"/> DELEGATED PERMISSIONS	
Access the directory as the signed-in user	<input type="radio"/> No
Read directory data	<input checked="" type="checkbox"/> Yes
Read and write directory data	<input checked="" type="checkbox"/> Yes
Read and write all groups	<input checked="" type="checkbox"/> Yes
Read all groups	<input checked="" type="checkbox"/> Yes
Read all users' full profiles	<input checked="" type="checkbox"/> Yes
Read all users' basic profiles	<input type="radio"/> No Activate W Go to Settings
Sign in and read user profile	<input type="radio"/> No

5. Enable the following access under delegated permissions in Power BI access.

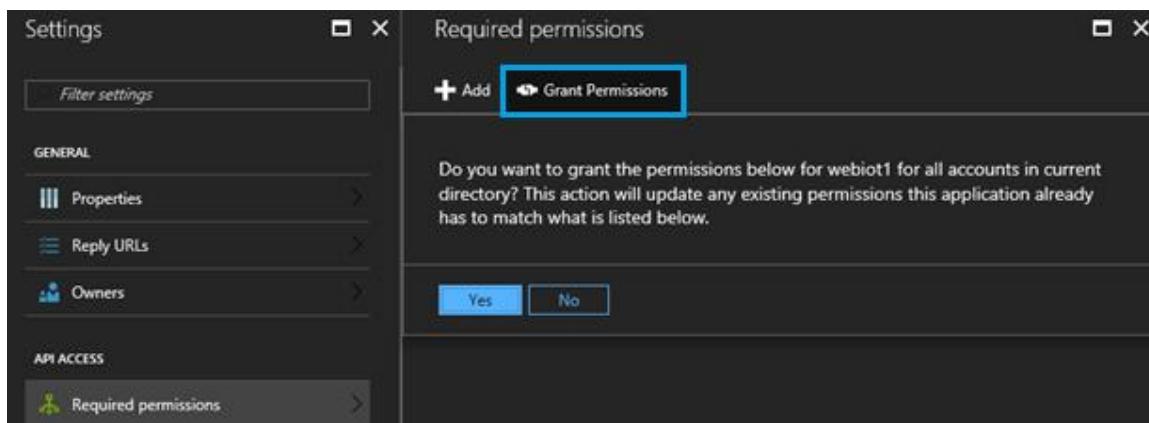
- View all datasets
- View all dashboards
- View content properties
- View all reports
- Create content
- View user groups
- Read and write all datasets
- Read and write all reports

The screenshot shows two adjacent Azure portal pages. On the left is the 'Required permissions' page, which lists 'API' entries for 'Power BI Service (Microsoft.Azure.AnalysisServices)' and 'Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)', both with 0 application permissions and 5 delegated permissions. On the right is the 'Enable Access' page for 'Microsoft Azure Analysis Services', showing a warning about adding permissions and a list of 8 delegated permissions selected with checkboxes. A blue box highlights the 'DELEGATED PERMISSIONS' section.

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

The screenshot shows the 'Settings' page for an application. Under 'API ACCESS', the 'Required permissions' section is highlighted with a blue box. It lists the same two APIs as the previous screen, with the total count of 8 delegated permissions highlighted by a blue box.

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



4.3. 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".

You're missing out on log analytics!

Enable Dynatrace log analytics to automatically correlate host-process log data with problems detected in your environment. Search log files for specific text patterns and create pattern-detection rules that trigger custom events.

Deploy Dynatrace

Log viewer demo

Here you can browse through the contents of individual process log files or search selected log files using keywords and filtering. Search queries can be saved and reused later. Log results can be returned in either raw or aggregated form.

Search for text patterns in selected log files using [advanced query language](#) (or leave blank to return all results).
For example, ("internal exception" OR error) AND NOT repeat*

Selected log files:

Hosts perspective	Type here to filter hosts, processes and log names	No logs selected, click below to select.
		CLOSE
> demo host	1 process.	3 log files
		58.6 kB

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

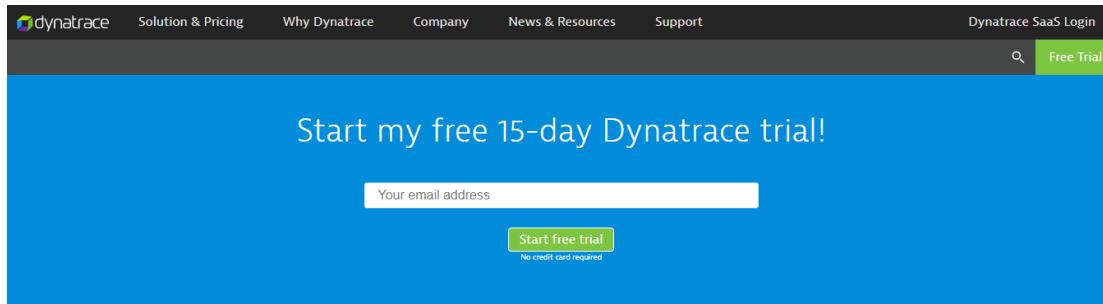
New Users: Please follow the below steps for "Sign up to Dynatrace trial SaaS for 15 days."

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>



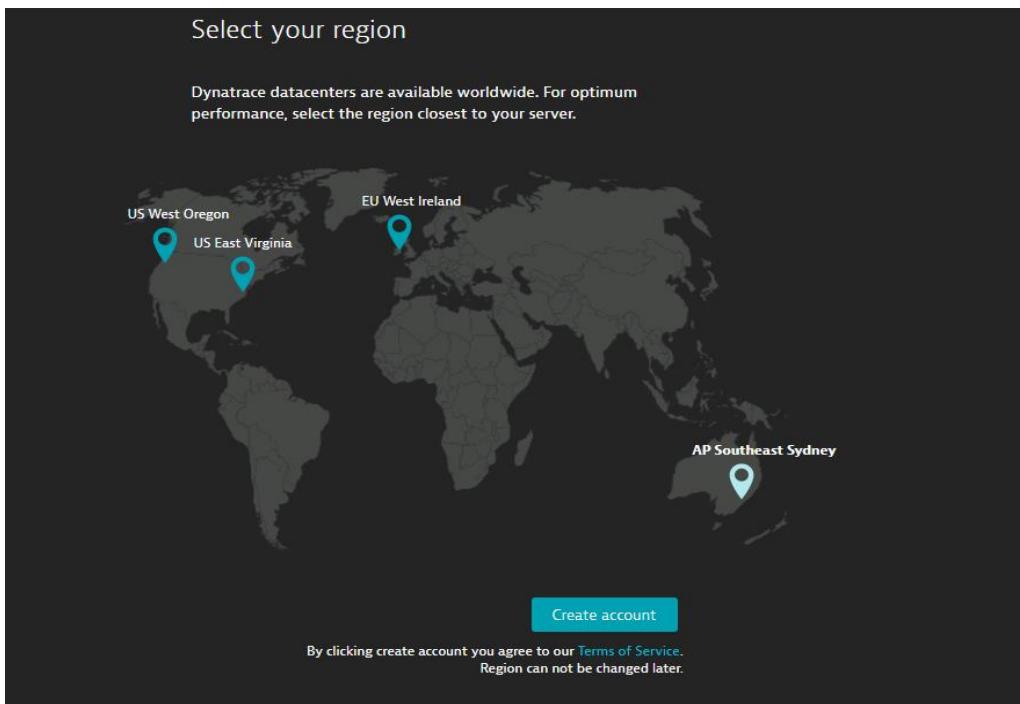
Get started now with Dynatrace SaaS or [contact us](#) for Dynatrace on-premises!



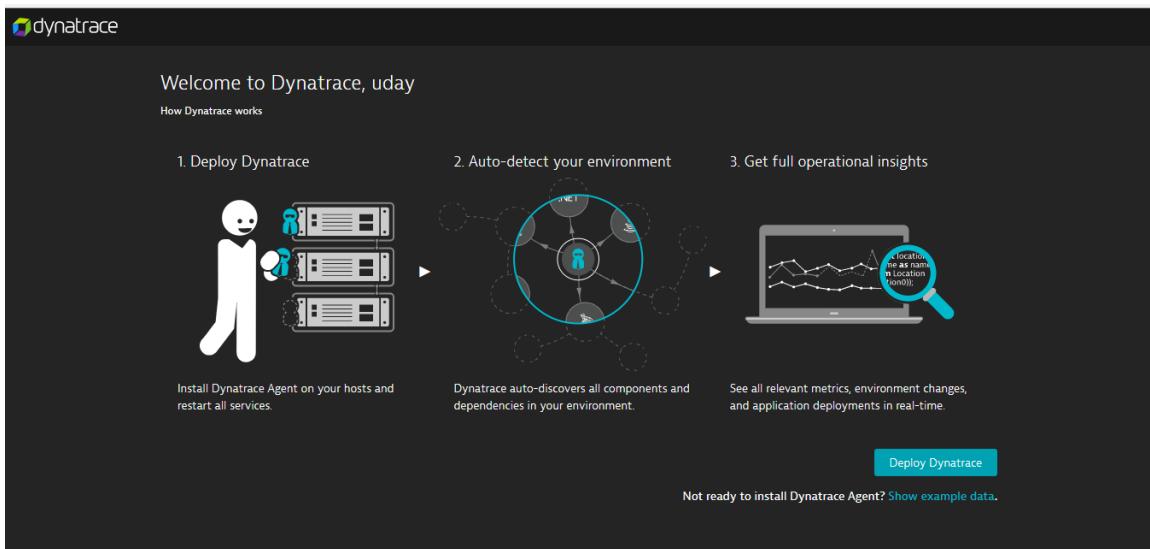
2. The below screen will appear. Fill out the **Create account**, **Account details** and **Select your region** screens.

A screenshot of the "Provide your account details" form. The form is part of a three-step process, with "Create account" and "Select your region" being the previous and next steps respectively. The "Account details" step is currently active, indicated by a blue underline. The form fields include: First name (input field), Last name (input field), Company (input field), Country (dropdown menu), Phone number (input field with placeholder "Optional"), Partner or promo code (input field with placeholder "Optional"), and a checkbox for "Tell me more about application performance".

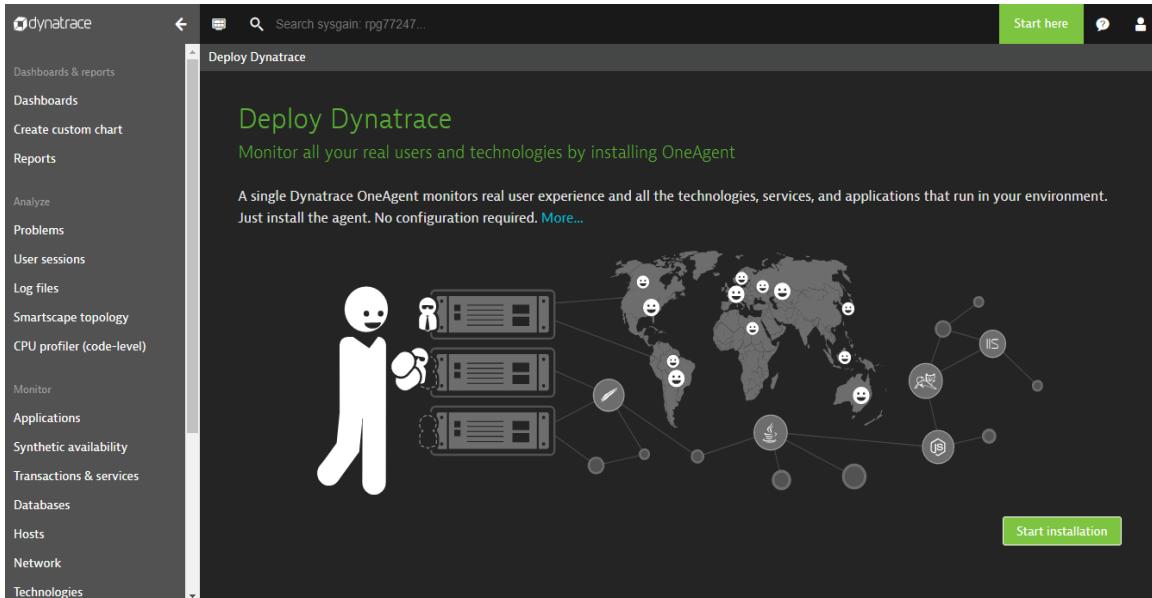
3. Select your region and click on “**Create account**”.



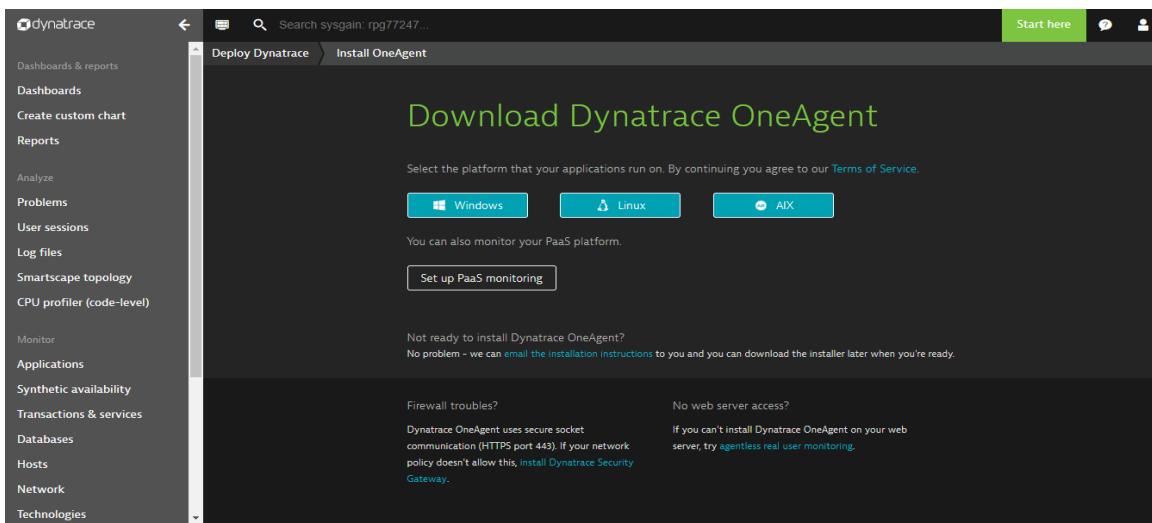
4. Click on “**Deploy Dynatrace**”.



5. Click on “**Start installation**”.



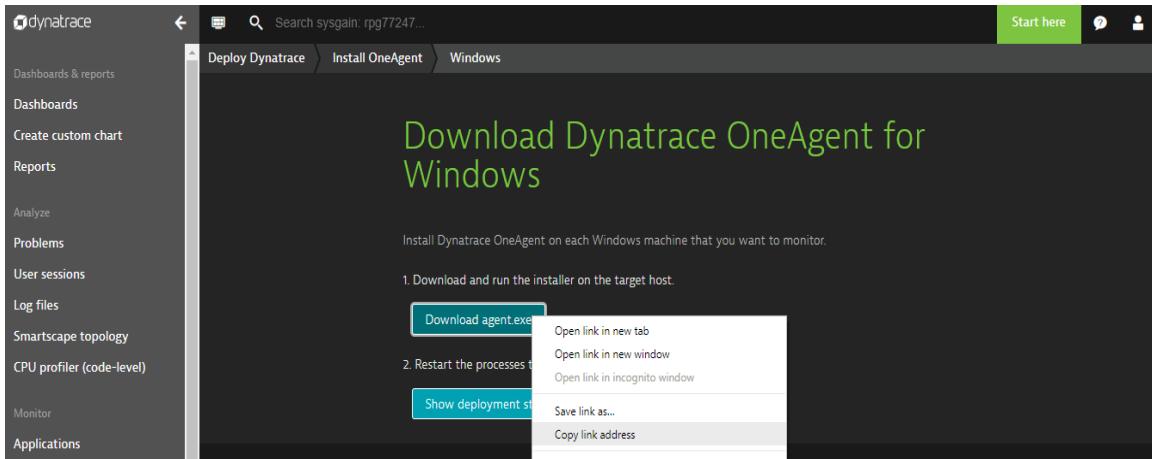
6. On the next screen, click "**Windows**".



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

E.g. URL -

<https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix>



5. Input Parameters

Parameter Name	Description	Allowed Values	Default Value
adminUsername	Admin username for all the deployed virtual machines	Any string	adminuser
adminPassword	Password to authenticate virtual machine	Password must be 12 characters and have 3 of the following 1 lower case character, 1 number, and 1 special character	
domainName	Domain names are used to identify one or more IP addresses.	Any domain names. (E.g. msfiot.com)	
websiteName	FQDN prefix for the application endpoint. Should be unique	Give the websitename used in the redirect URL during the webapplication creation(E.g : give 'iotwebsite' from https://iotwebsite.azurewebsites.net/redirect.html	
sqlAdministratorLogin	The SQL authentication admin user of the Azure SQL Server	Any string	sqluser

sqlAdministratorLoginPassword	The SQL authentication password of the admin user of the Azure SQL Server	Password must be 12 characters and have 3 of the following 1 lower case character, 1 number, and 1 special character	
skuName	App service plan's pricing tier and instance size. More information - https://azure.microsoft.com/en-us/pricing/details/app-service/	D1, B1, B2, B3, S1, S2, S3, P1, P2, P3, P4	S1
skuCapacity	App service plan's pricing instance count	minValue – 1 maxValue - 4	1
emailHost	Describes the host name for sending email notifications	Any string	
emailHostPort	Describes the port number for email host	Range	25
senderEmail	Describes the email ID of the sender for email notifications.	Email format. (E.g. iot@microsoft.com)	
senderEmailPassword	Describes the password for the sender email ID for email notifications.	Valid password string	
b2cTenant	Azure Active Directory B2C is a cloud identity service allowing you to connect to any customer. Describes B2C tenant name directory.	Valid B2C tenant. (E.g. iot.onmicrosoft.com)	
b2cClientId	Describes the client Id of the application registered in B2C directory.	GUID	
b2cClientSecret	Describes the Client secret of the application registered in B2C directory.		
b2cSignUpPolicyId	Sign-up policy allows you to control behaviors by configuring the Account types and Attributes. This field is the id for the B2C Sign up policy	Valid B2C sign up policy. (E.g. B2C_1_suppolicy2)	
b2cSignInPolicyId	Describes the B2C Sign in policy	Valid B2C sign in policy. (E.g. B2C_1_sinpolicy2)	
b2cEditProfilePolicyId	Describes the B2C Profile Editing policy.	Valid B2C Profile Editing policy. (E.g. B2C_1_peditpolicy2)	

b2cChangePasswordPolicy	Describes the B2C Change Password policy.	Valid B2C Change Password policy. (E.g. B2C_1_cpasspolicy)	
MLskuName	Pricing tier for machine learning workspace.	S1, S2, S3	S1
chefUserFirstName	First name of the Chef user.	Any string	
chefUserLastName	Last name of the Chef user.	Any string	
chefuserEmail	Email of the Chef user.	Valid email address (E.g. orguser@noone.com)	
chefOrgShortname	Short name of the Chef's organization	Any string	

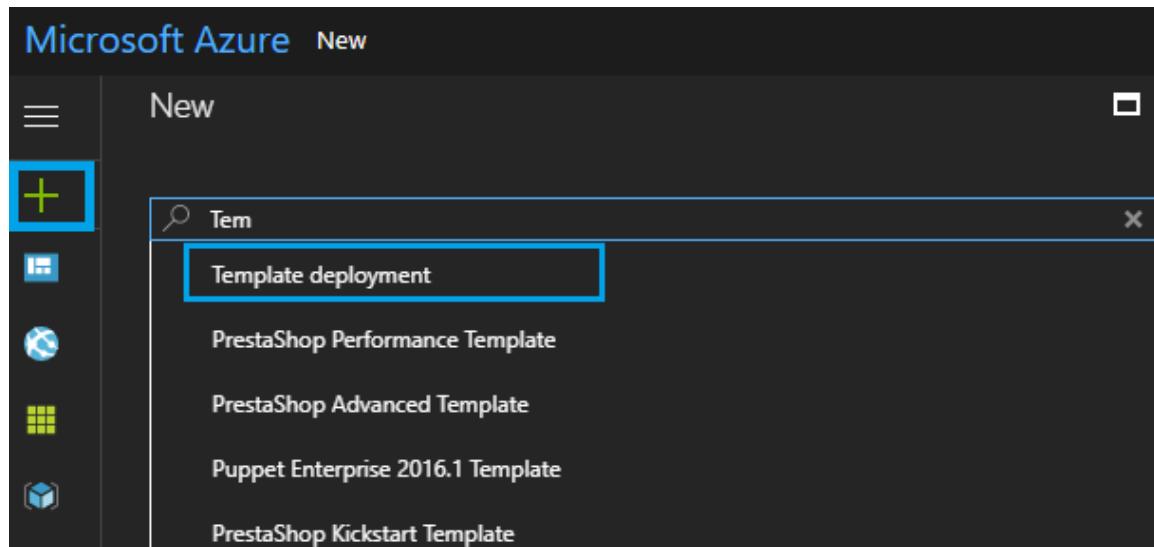
6. Azure Resource Manager Template Deployment

Click on below Git hub repo url

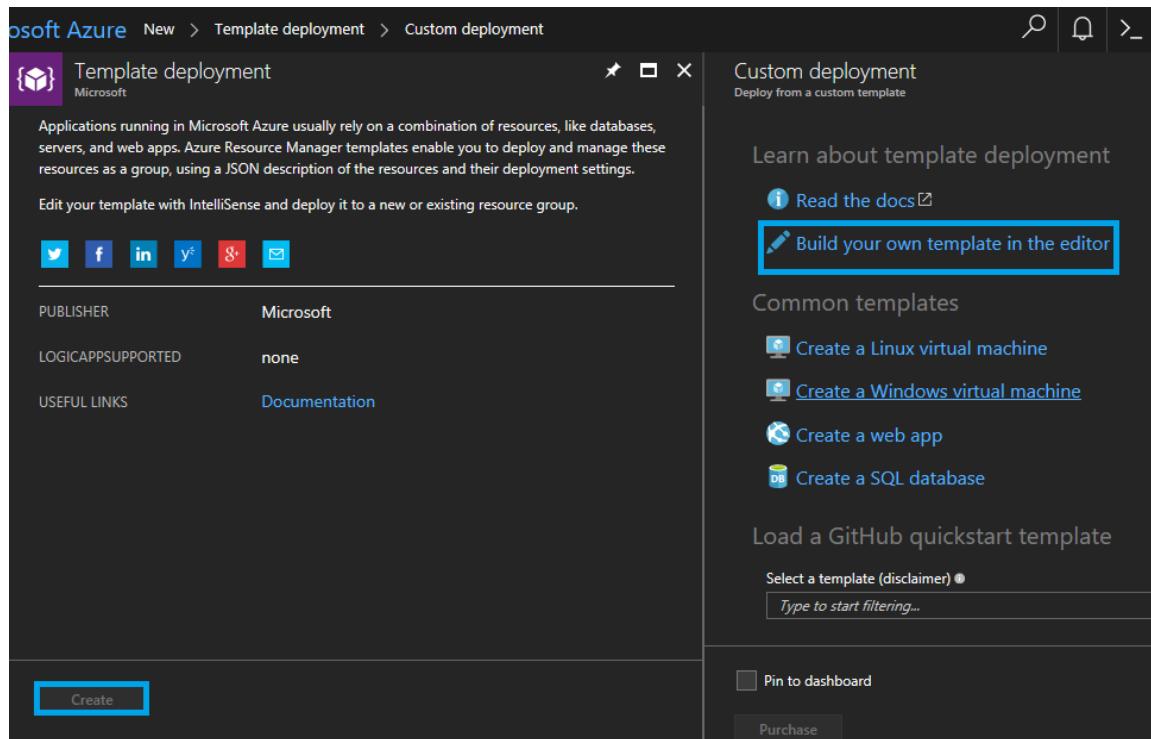
<https://github.com/sysgain/iot-automation/tree/sysgainiot>

Take the maintemplate.json raw

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

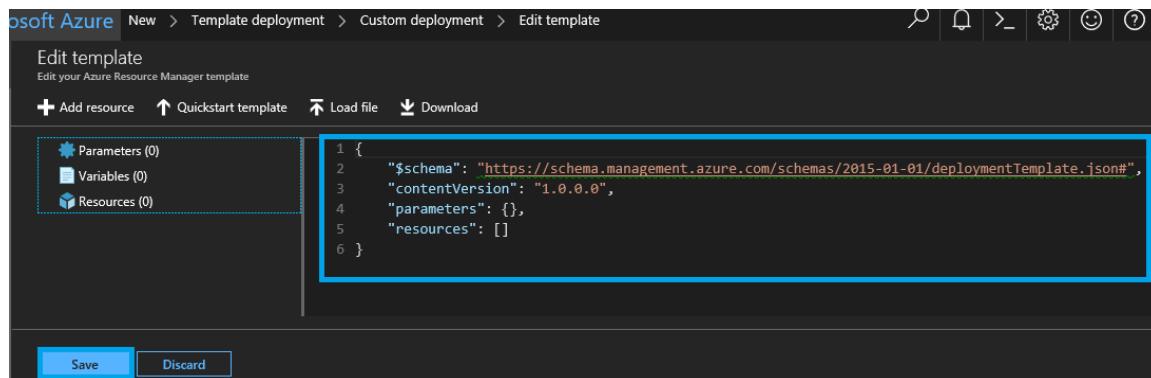


2. Click on **create** and click on **Build your own Template**.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'New', 'Template deployment', and 'Custom deployment'. The main content area is titled 'Template deployment' under 'Microsoft'. It contains a brief description of Azure Resource Manager templates and a section for editing the template with IntelliSense. Below this are publisher information ('Microsoft'), logic app support ('none'), and useful links ('Documentation'). A large 'Create' button is at the bottom left. On the right side, there's a sidebar titled 'Custom deployment' with a sub-section 'Learn about template deployment' containing 'Read the docs' and 'Build your own template in the editor' (which is highlighted with a blue border). Other sections include 'Common templates' (with links to 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', and 'Create a SQL database') and 'Load a GitHub quickstart template' with a search bar.

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



The screenshot shows the 'Edit template' blade in the Azure portal. The top navigation bar includes 'New', 'Template deployment', 'Custom deployment', and 'Edit template'. The main content area is titled 'Edit template' with the sub-instruction 'Edit your Azure Resource Manager template'. It features a toolbar with 'Add resource', 'Quickstart template', 'Load file', and 'Download'. On the left, there are three collapsed sections: 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main pane displays the JSON template code, which is highlighted with a blue border. The code starts with a schema reference and ends with a closing brace. At the bottom, there are 'Save' and 'Discard' buttons, with 'Save' being highlighted with a blue border.

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

Admin Username ⓘ	<input type="text" value="adminuser"/>
Admin Password ⓘ	<input type="password" value="*****"/>
Domain Name ⓘ	<input type="text" value="sysgainiot.com"/>
Bastion VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
Chef Workstation VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
Fortigate VM Size ⓘ	<input type="text" value="Standard_D1_v2"/> ▼
Ad Server VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
Trend VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
Splunk VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
Chef Automate VM Size ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
PIAFDASQL Server VMSize ⓘ	<input type="text" value="Standard_DS2_v2"/> ▼
PIBA Server VMSize ⓘ	<input type="text" value="Standard_DS4_v2"/> ▼
Website Name	<input type="text" value="webtest"/>
Sql Administrator Login ⓘ	<input type="text" value="sqluser"/>

Sql Administrator Login Password ⓘ	*****
Sku Name ⓘ	S1
Sku Capacity ⓘ	1
Email Host ⓘ	iothost
Email Host Port ⓘ	25
Sender Email ⓘ	sender@noreply.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@noreply.com
Chef Org Short Name ●	chefforg

TERMS AND CONDITIONS

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

5. Once all the parameters are entered click on **Purchase**.
6. After launching the template, the following resources will be created in a Resource Group:
 - 2 App Services
 - 1 App service plan
 - 1 work space plan and work space in Machine Learning
 - 8 Network interfaces
 - 8 network security groups
 - 3 public IP address
 - 1 scheduler job collection
 - 2 SQL databases
 - 2 SQL Servers
 - 8 storage accounts
 - 8 disks

- 8 virtual machines
- 1 Virtual network

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

The screenshot shows the Azure portal interface for managing resources. On the left, there's a sidebar with navigation links like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, and Automation script. The main area displays a list of virtual machines under the 'Essentials' section. The list includes columns for NAME, TYPE, and LOCATION. A blue box highlights the first seven items in the list:

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	wsclientsstnh6.southindia.cloudapp.azure.com	
CHEFAUTOMATEIPADDRESS	10.0.1.6	
CHEFAUTOMATELOGINUSERN...	adminuser	
TRENDIPADDRESS	10.0.1.10	
TRENDWEBUIUSERNAME	adminuser	
SPLUNKIPADDRESS	10.0.1.8	

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

7. Security And Monitoring Components

Bastion Host: 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 tries to ensure that the files and software we are expecting to be on a machine 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 and 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 Public IP Address provided in the output section.



Remote Desktop Connection



Remote Desktop Connection

Computer:

13.84.158.183



User name: None specified

You will be asked for credentials when you connect.

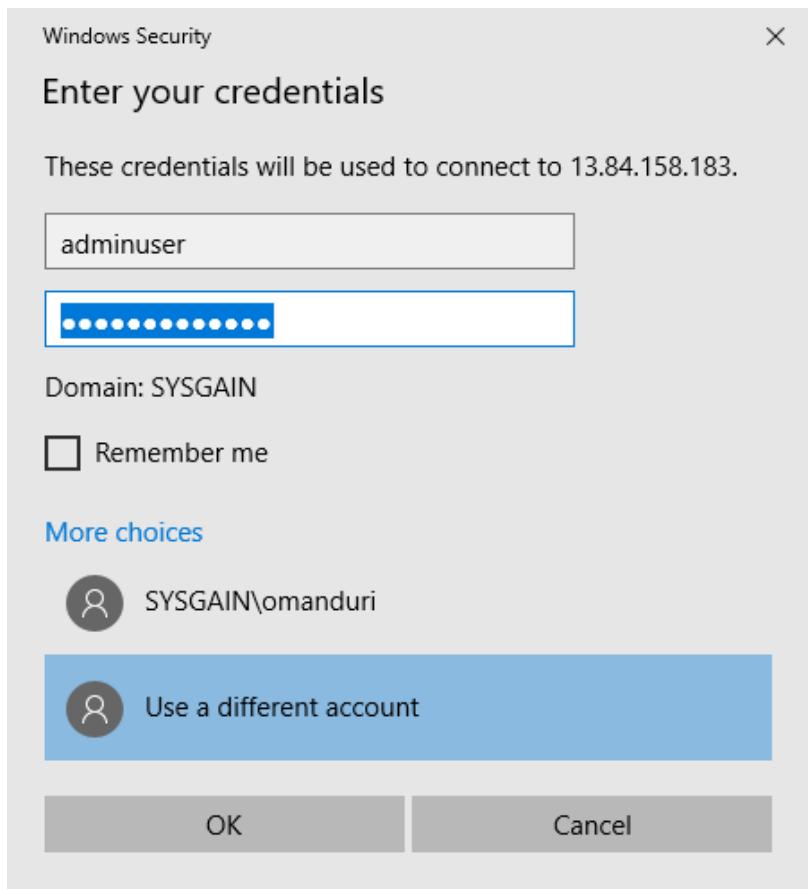


Show Options

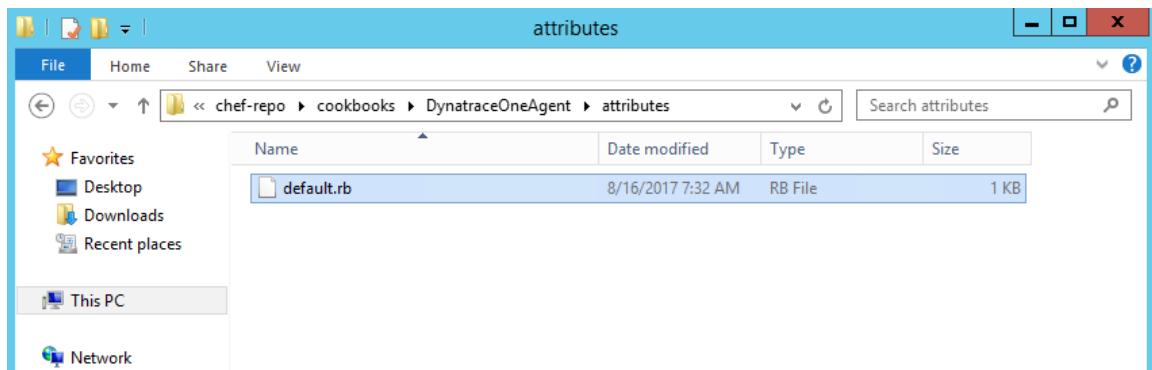
Connect

Help

2. Enter the credentials provided in the output section.

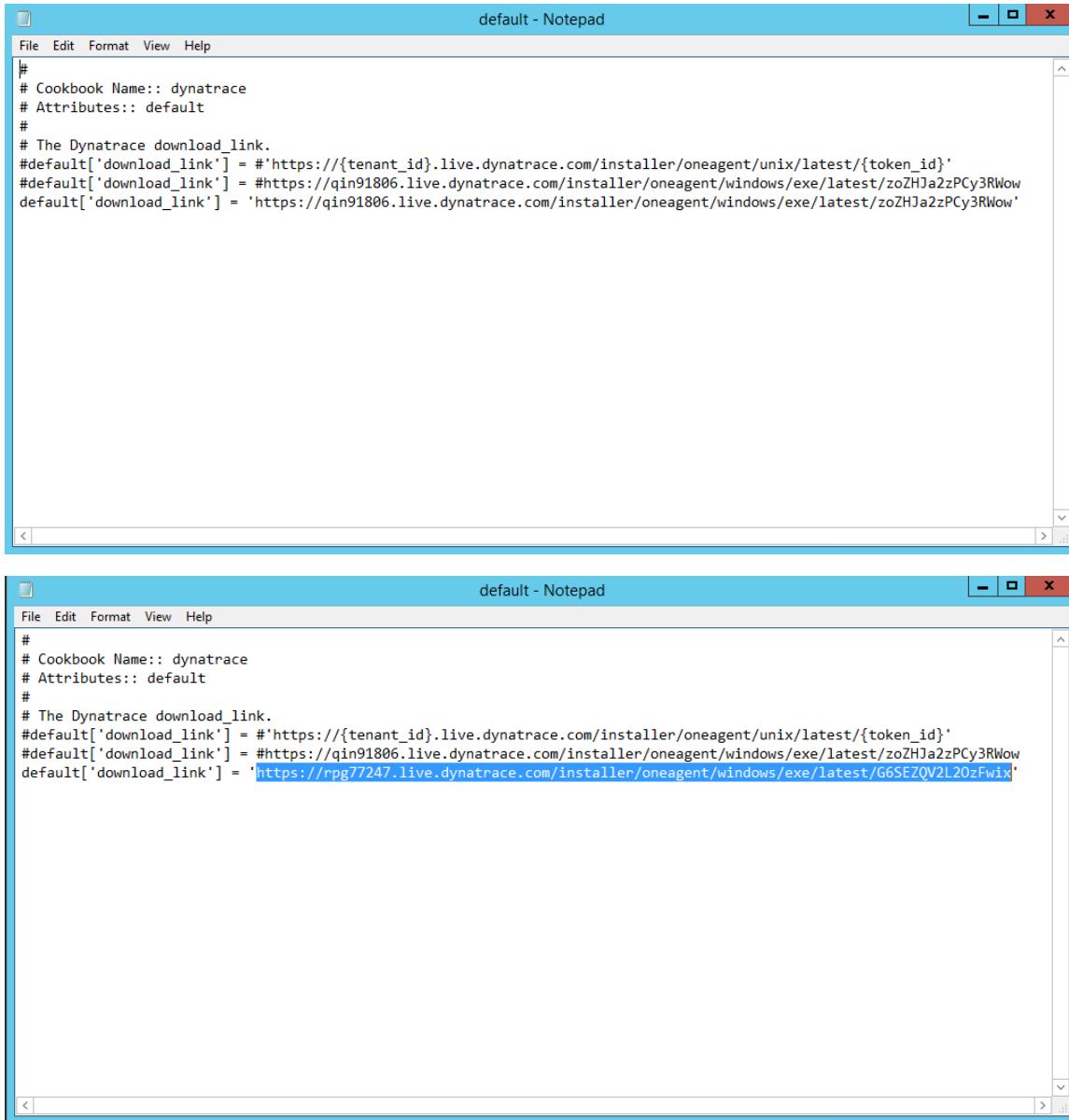


2. After logging in, navigate to **C:\Users\chef-repo\cookbooks\DynatraceOneAgent\attributes** and open the **default.rb** file.



3. Add the new unique url:

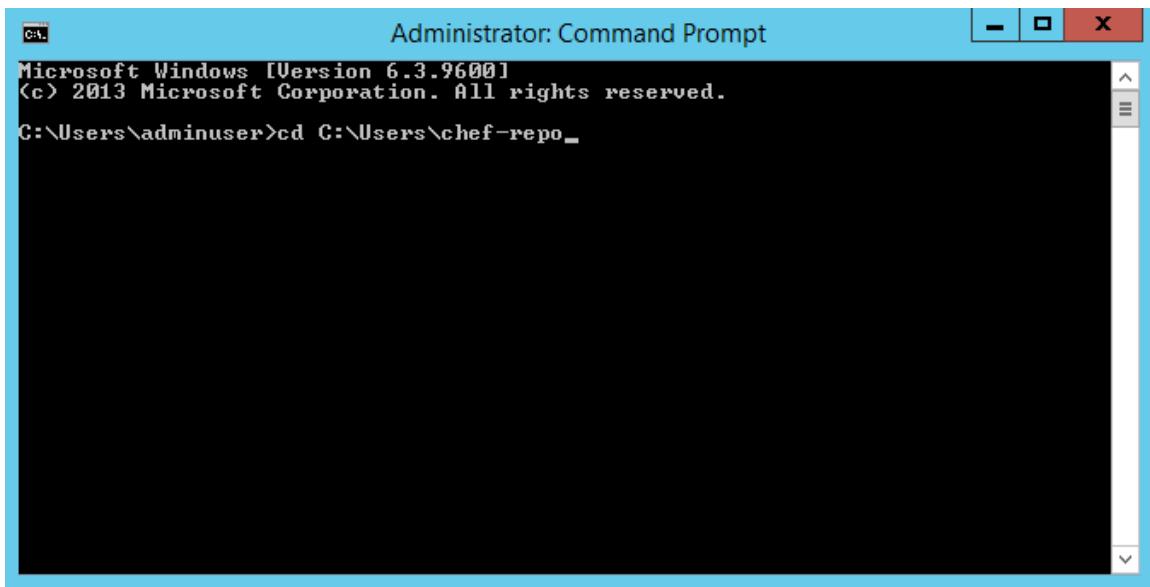
<https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix> as the last link and **save** the file.



The image shows two identical windows titled "default - Notepad". Both windows display the same Chef cookbook configuration code. The code defines a cookbook named "dynatrace" with default attributes. It includes a comment for the Dynatrace download link and three default download link options. The last option, which is highlighted in blue, is the new unique URL provided in the instructions: "https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix".

```
#  
# Cookbook Name:: dynatrace  
# Attributes:: default  
#  
# The Dynatrace download_link.  
#default['download_link'] = #'https://{{tenant_id}}.live.dynatrace.com/installer/oneagent/unix/latest/{{token_id}}'  
#default['download_link'] = #https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow  
default['download_link'] = 'https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow'  
  
#  
# Cookbook Name:: dynatrace  
# Attributes:: default  
#  
# The Dynatrace download_link.  
#default['download_link'] = #'https://{{tenant_id}}.live.dynatrace.com/installer/oneagent/unix/latest/{{token_id}}'  
#default['download_link'] = #https://qin91806.live.dynatrace.com/installer/oneagent/windows/exe/latest/zoZHJa2zPCy3RWow  
default['download_link'] = 'https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix'
```

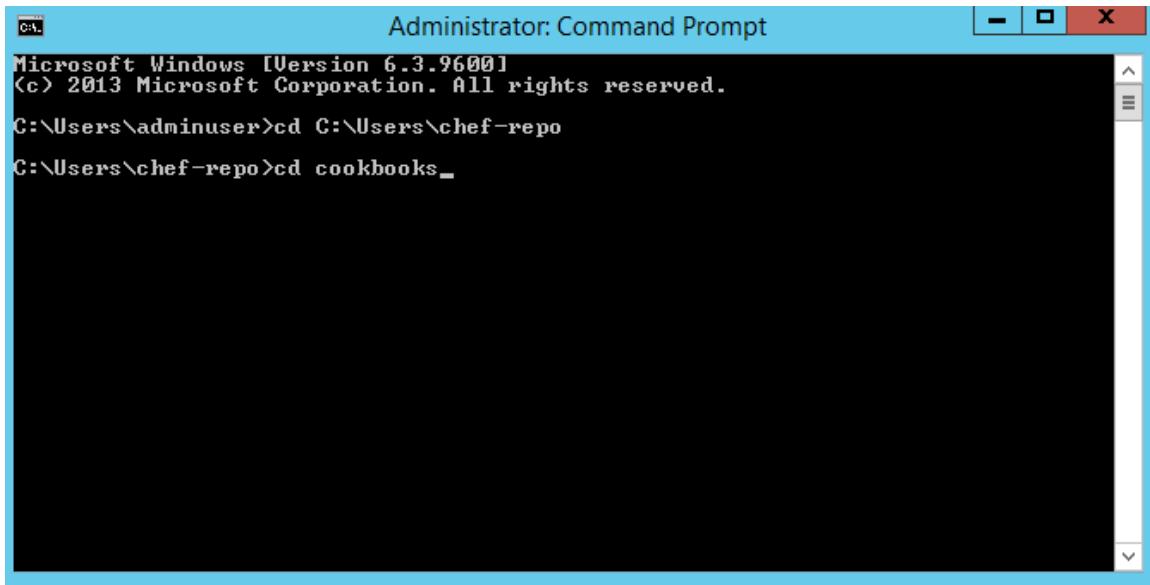
4. Open the command prompt and navigate to "**chef-repo**".



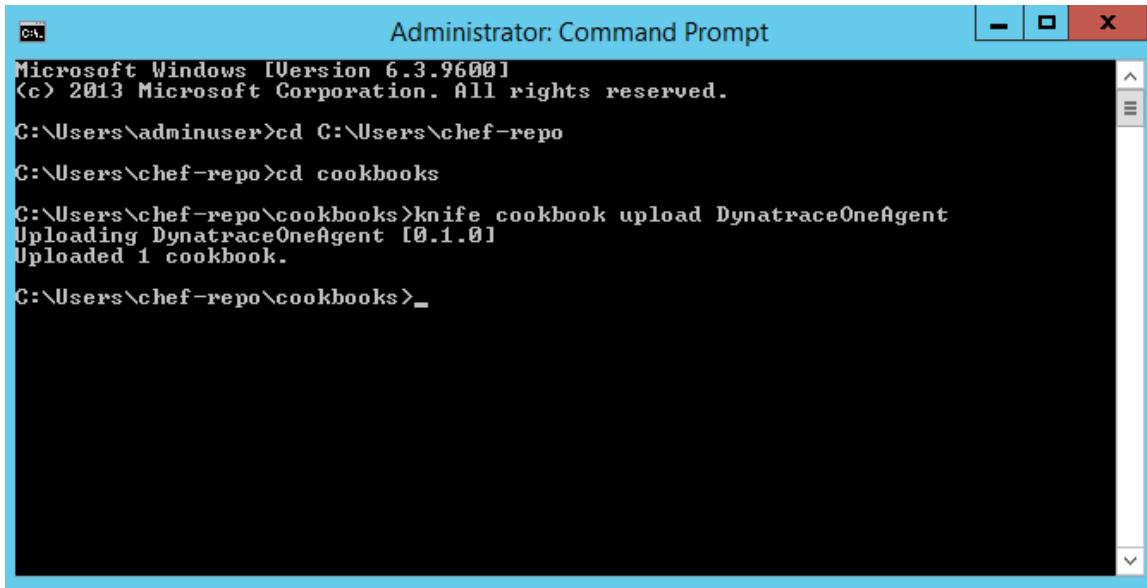
```
C:\ Administrator: Command Prompt Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. All rights reserved. C:\Users\adminuser>cd C:\Users\chef-repo_
```

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

```
knife cookbook upload DynatraceOneAgent
```



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



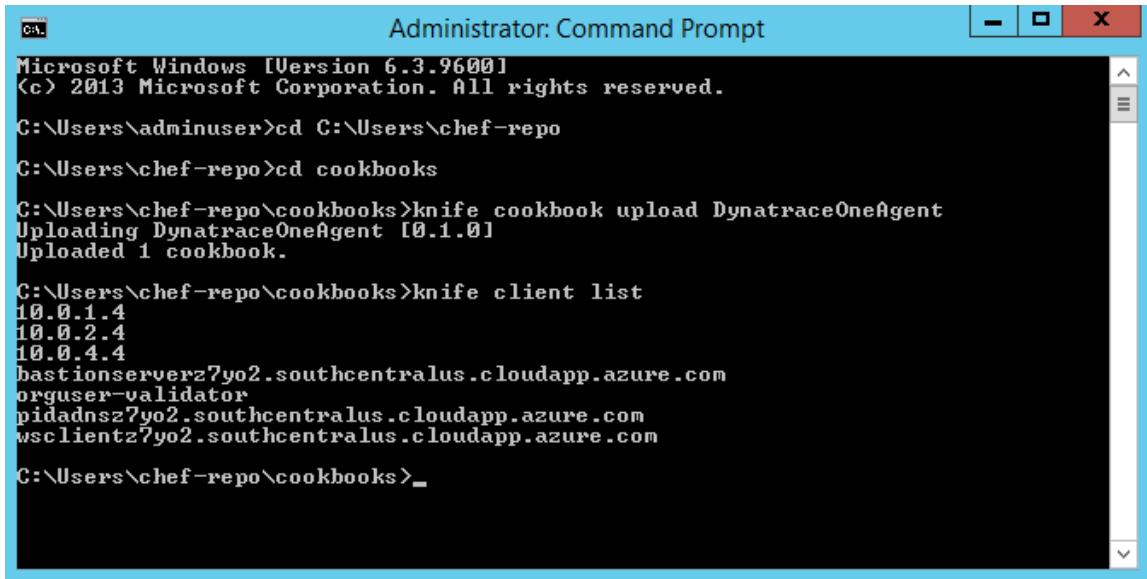
```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

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

```
| knife client list
```



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

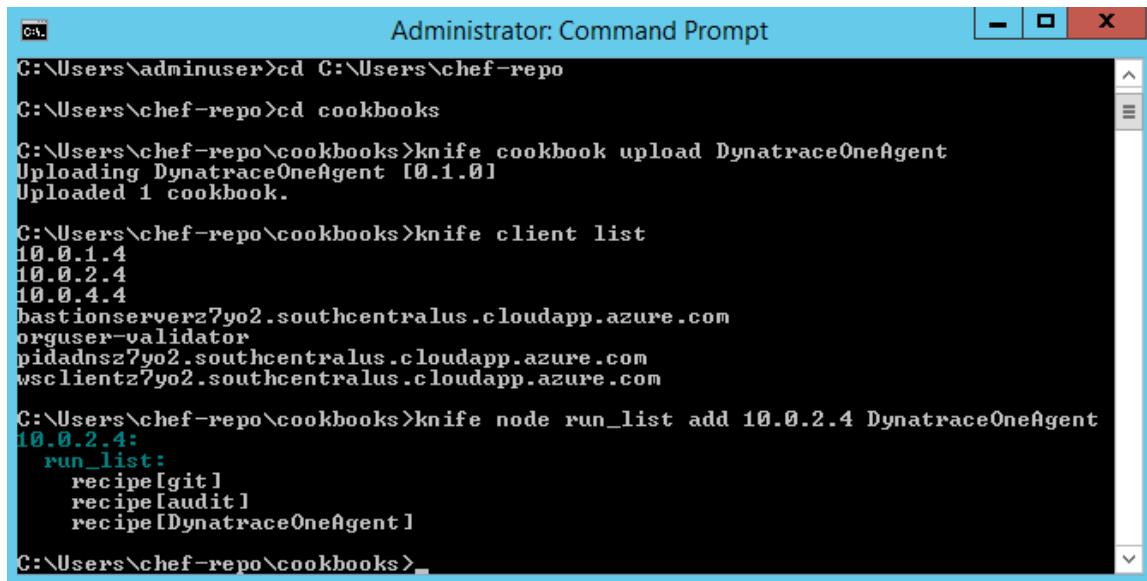
C:\Users\adminuser>cd C:\Users\chef-repo
C:\Users\chef-repo>cd cookbooks
C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

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

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

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



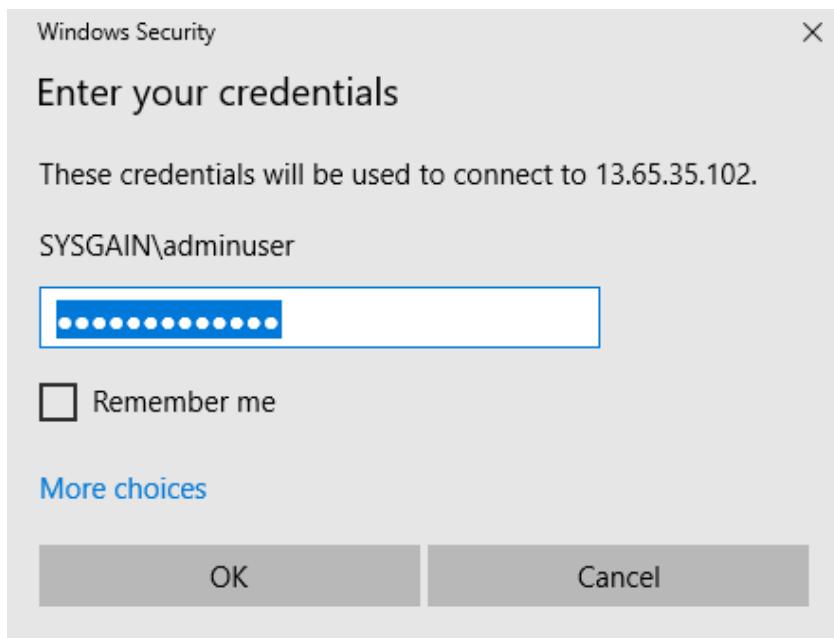
```
Administrator: Command Prompt
C:\Users\adminuser>cd C:\Users\chef-repo
C:\Users\chef-repo>cd cookbooks
C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

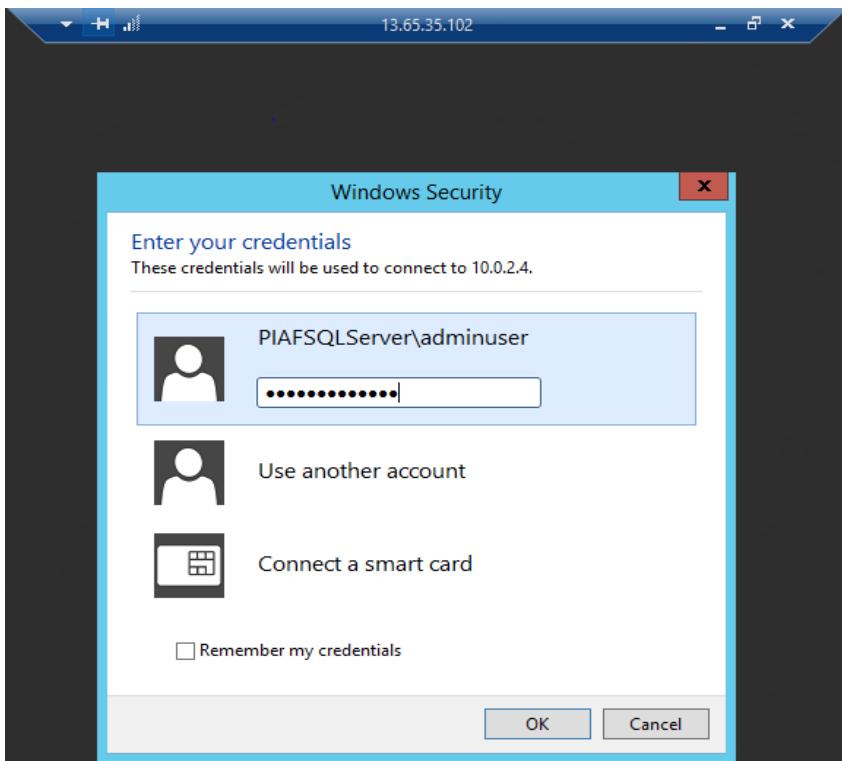
C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserverz7yo2.southcentralus.cloudapp.azure.com
orguser-validator
pidadnsz7yo2.southcentralus.cloudapp.azure.com
wsclientz7yo2.southcentralus.cloudapp.azure.com

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>
```

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





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

A screenshot of an Administrator Command Prompt window titled "Administrator: Command Prompt" on a Windows 10 desktop. The taskbar shows the IP address "10.0.2.4". The command line shows the user running "C:\Users\admininuser>chef-client".

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

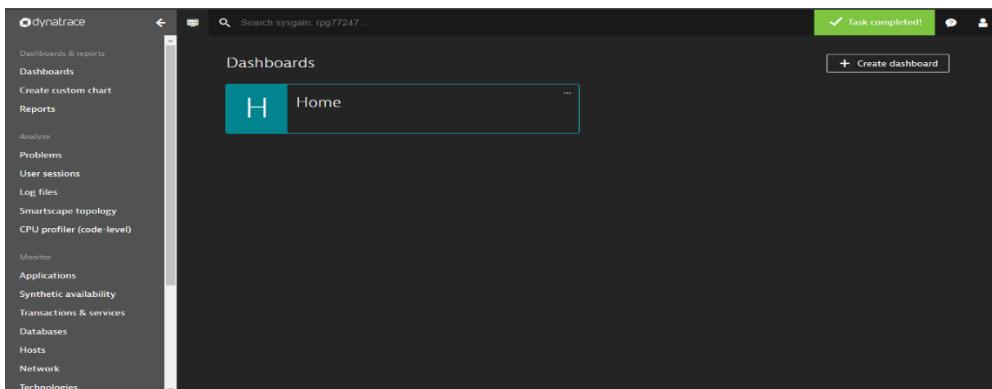
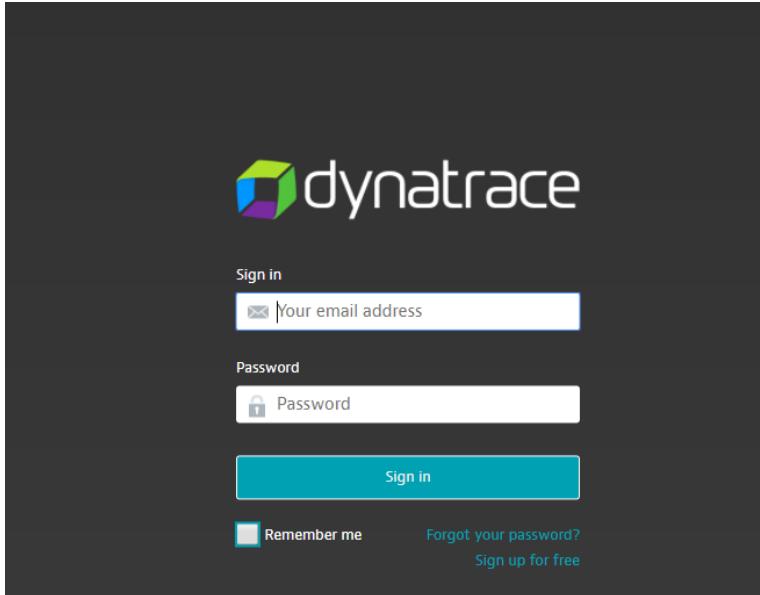
```
- install version latest of package DynatraceOneAgent
* windows_service[Dynatrace OneAgent] action restart[2017-08-16T14:10:56+00:00] INFO: Processing windows_service[Dynatrace OneAgent] action restart (DynatraceOneAgent::oneagent-windows line 28)
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace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

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

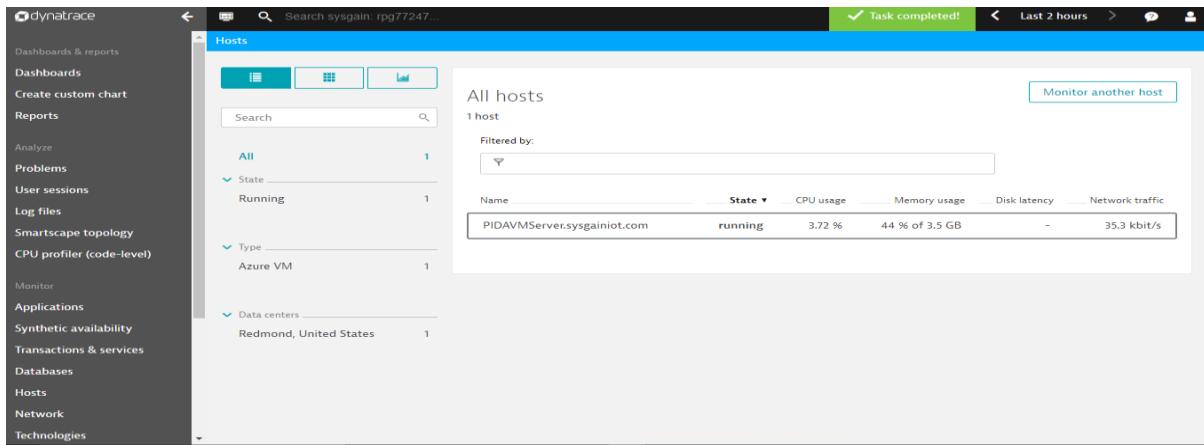
Running handlers:
[2017-08-16T14:11:09+00:00] INFO: Running report handlers
[2017-08-16T14:11:11+00:00] WARN: Format is json
[2017-08-16T14:11:11+00:00] INFO: Initialize InSpec 1.30.0
[2017-08-16T14:11:12+00:00] INFO: Running tests from: [{:name=>"windows-baseline", :git=>"https://github.com/dev-sec/windows-baseline"}]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

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

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



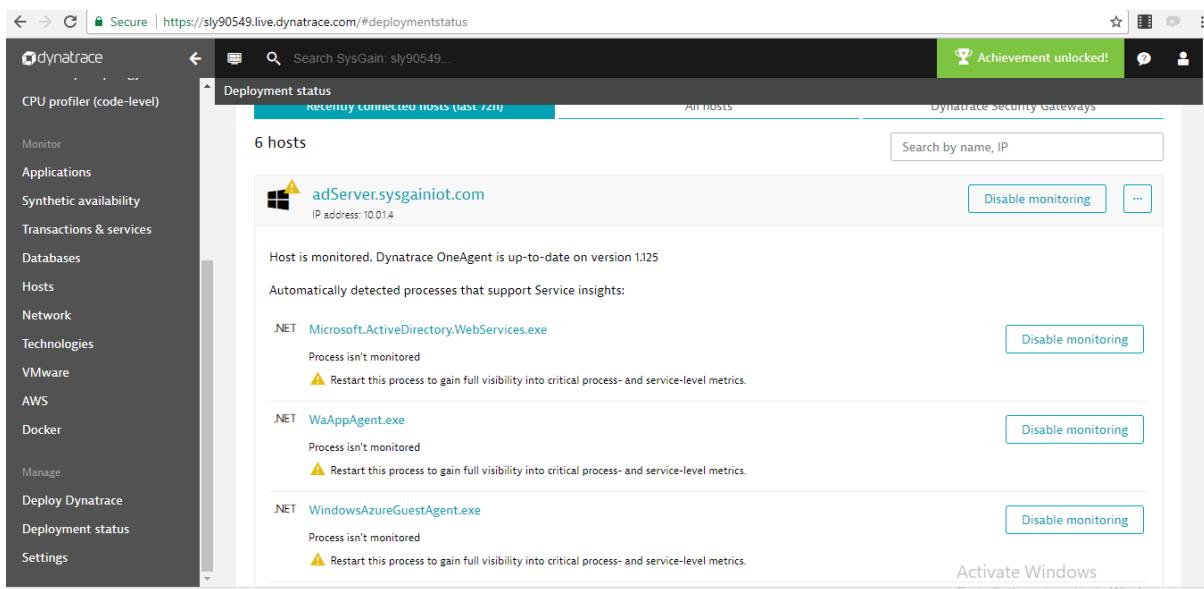
12. From the left side menu select “**Host**”. Here you can see the target host added to the Dynatrace Dashboard.



The screenshot shows the Dynatrace Hosts dashboard. On the left sidebar, under the "Monitor" section, the "Hosts" option is selected. The main area displays a table titled "All hosts" with one entry: "PIDAVMServer.sysgainiot.com" which is "running". The table includes columns for Name, State, CPU usage, Memory usage, Disk latency, and Network traffic. A "Monitor another host" button is located in the top right corner 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 dashboard. On the left sidebar, the "Deployment status" option is selected. The main area displays a table titled "6 hosts" with one entry: "adServer.sysgainiot.com" (IP address: 10.0.1.4). The table lists three processes: Microsoft.ActiveDirectory.WebServices.exe, WaAppAgent.exe, and WindowsAzureGuestAgent.exe. Each process has a "Disable monitoring" button and a note indicating it is not monitored and suggesting a restart. A "Search by name, IP" input field is at the top right, and an "Activate Windows" link is at the bottom right.

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

The screenshot shows the Dynatrace interface with the URL <https://sly90549.live.dynatrace.com/#deploymentstatus>. The left sidebar includes options like CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main content area displays the 'Deployment status' for host RD00155DA9BEC5 with IP address 100.69.152.36. It lists automatically detected processes: EnergyManagementScheduler.WebJob.exe (J.NET), IIS app pool apiservergop4 (IIS), IIS app pool webiotivivek (IIS), IIS app pool ~apiservergop4 (IIS), and IIS app pool ~webiotivivek (IIS). Each process entry has a 'Disable monitoring' button. A green banner at the top right says 'Achievement unlocked!' with a gear icon. A small message 'Activate Windows' is visible at the bottom right.

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.

The screenshot shows the Dynatrace interface with the URL <https://sysgain:rpg77247@live.dynatrace.com/#hosts>. The left sidebar includes options like Dashboards & reports, Dashboards, Create custom chart, Reports, Analyze, Problems, User sessions, Log files, Smartscape topology, CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, and Technologies. The main content area shows the 'Hosts' page for PIDAVMServer.sysgainiot.com, which has been up for 1 day 1 hour 54 minutes. It displays system properties: Windows Server 2012 R2, ver. 6.3.9600. A summary bar shows 100% Availability with 0 min total downtime. Below this is a chart titled 'CPU usage 0.29 %' showing CPU usage over time from 13:30 to 15:00. A separate section titled 'Processes' lists .NET processes: pialink.exe, ServerManager.exe, SMTHost.exe, WaAppAgent.exe, WindowsAzureGuestAgent.exe, and WindowsAzureTelemetryService.exe. A blue button 'All processes' is at the bottom right of this section.

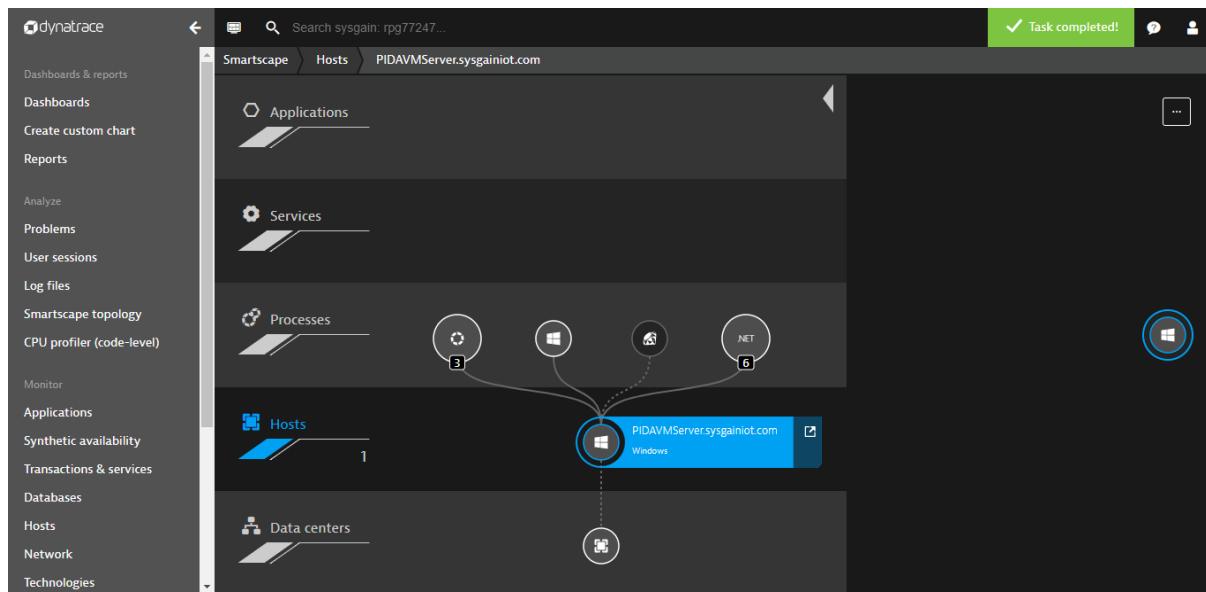
15. Click on “**All processes**”, to view the process details running on the host.

The screenshot shows the Dynatrace interface with a sidebar on the left containing various monitoring categories like Dashboards, Reports, Analyze, Problems, Applications, and Network. The main area displays a table titled "Processes" for the host "PIDAVMServer.sysgainiot.com". The table columns include Process, Type, CPU, Memory, Traffic, Retransmissions, and Connectivity. Processes listed include Deep Security Agent, OneAgent log analytics, Windows System, ServerManager.exe, OneAgent network monitoring, Remote Desktop Connection, piaflink.exe, OneAgent monitoring extensions, oneagentupdater.exe, WindowsAzureTelemetryService.exe, SMTHost.exe, chef-client, and WaAppAgent.exe. The "Deep Security Agent" process is highlighted with a blue background.

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 with the "Smartscape topology" view selected. The left sidebar includes "Dashboards", "Reports", "Analyze", "Problems", "User sessions", "Log files", "Smartscape topology", and "Monitor". The main area shows a summary for the host "PIDAVMServer.sysgainiot.com" with an uptime of "1 day 2 hours 1 minute". It features a "Properties" section with "Windows Server 2012 R2, ver. 6.3.9600" and a "CPU usage 0.21%" chart. To the right, there's a "No problems in last 72 hours" section and a "100% Availability" chart showing "0 min total downtime" from 14:00 to 15:00. A legend indicates "Running" (blue) and "Unmonitored" (yellow). Below these are sections for "Processes" and "Applications".



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

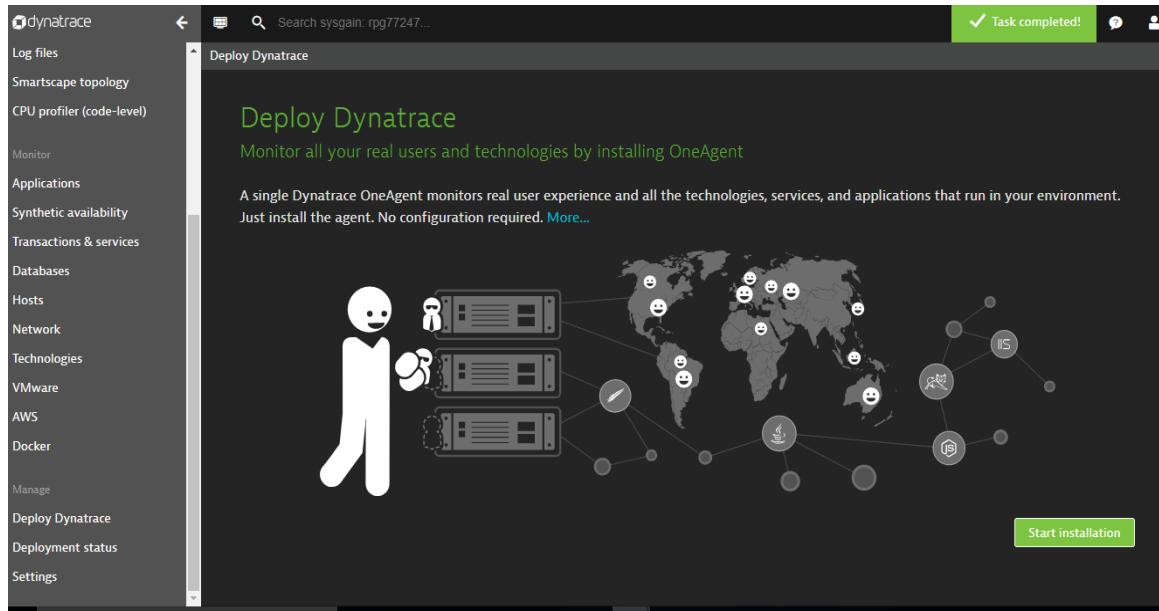
Azure Web Apps is a service provided by Microsoft Azure that gives you the option of deploying and auto-scaling applications and services. Using a predefined Azure site extension, you can modify your deployment by supplying additional resources or packages.

Generate a PaaS token:

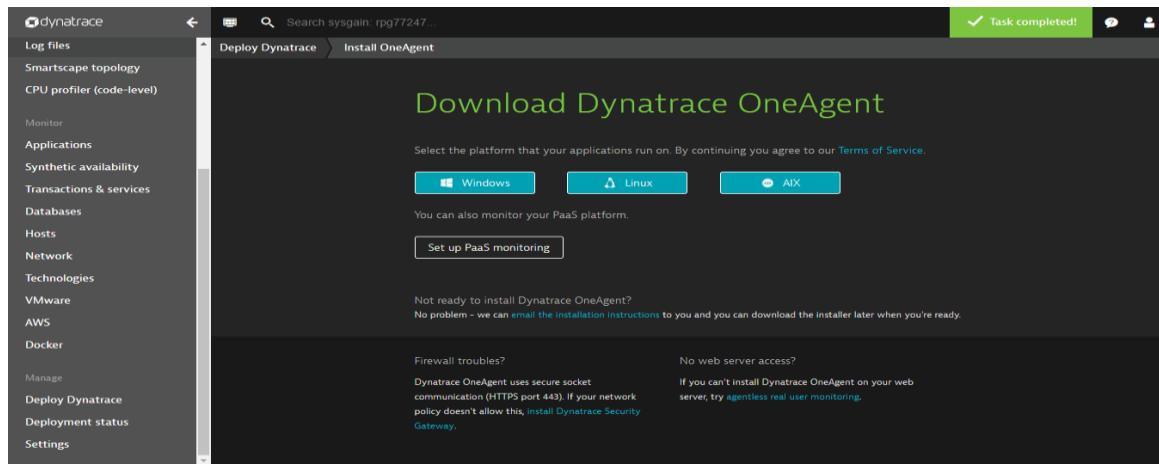
The first step is to get your environment ID and generate a PaaS token for your Dynatrace environment. This information is required so we can map your Azure account to your Dynatrace account.

To get your Dynatrace environment ID and PaaS token:

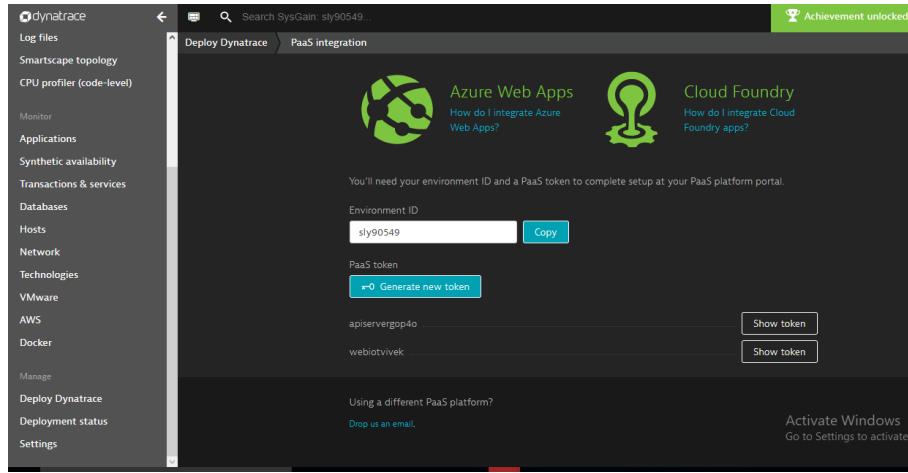
1. Login with your [Dynatrace account](#).
2. Select Deploy Dynatrace from the navigation menu.



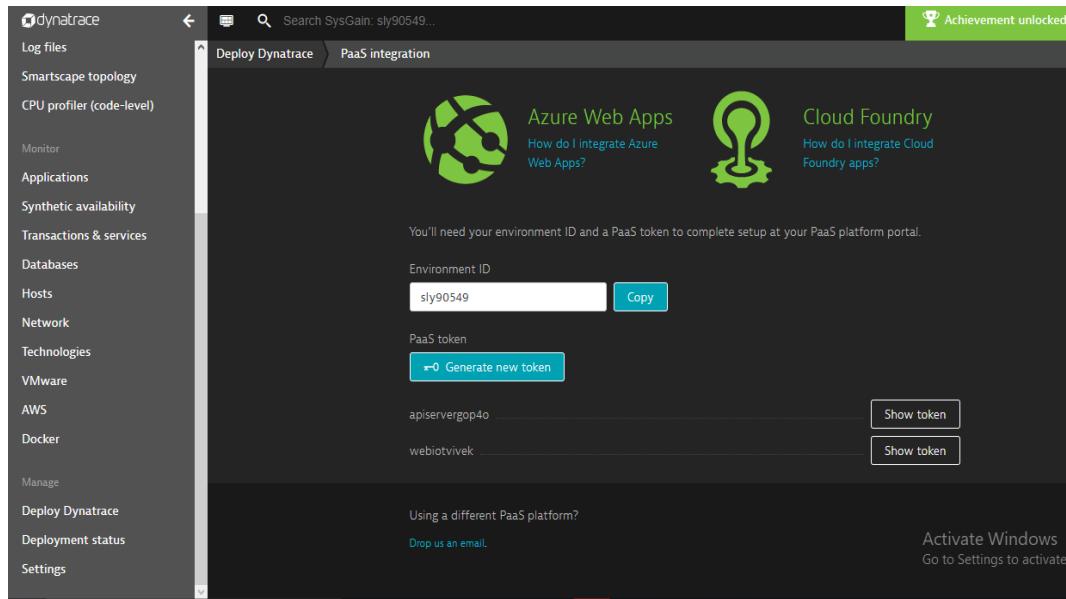
3. Click **Setup PaaS monitoring**.



- 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".

- 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

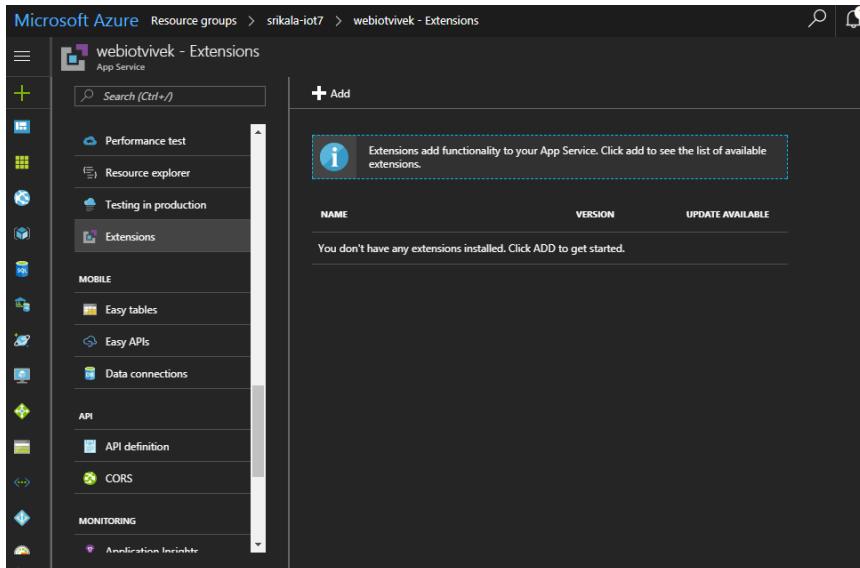
- Now, open **portal.azure.com** in a new browser window.
- Navigate to the web app in the resource group you want to monitor.
- From **Settings**, select **Application Settings**. Then, scroll down to the App Settings area and add two new **Key/Value** pairs:
- DT_TENANT**: Your environment ID, as shown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

Key	Value	Slot setting
restServer	https://apiserververgop40.azurewebsites.net/	<input type="checkbox"/>
b2cApplicationId	adf51569-fd45-431f-82e3-f72bfe0ee4a6	<input type="checkbox"/>
signInPolicyName	B2C_1_simplpolicy2	<input type="checkbox"/>
signInSignUpPolicyName	B2C_1_supplpolicy2	<input type="checkbox"/>
editProfilePolicyName	B2C_1_peditpolicy2	<input type="checkbox"/>
tenantName	testiot22.onmicrosoft.com	<input type="checkbox"/>
redirect_uri	https://webiotivivek.azurewebsites.net/#/dashboard	<input type="checkbox"/>
DT_TENANT	sly90549	<input type="checkbox"/>
DT_API_TOKEN	3o2WgxoYSH6-9y5NX2GS-	<input type="checkbox"/>

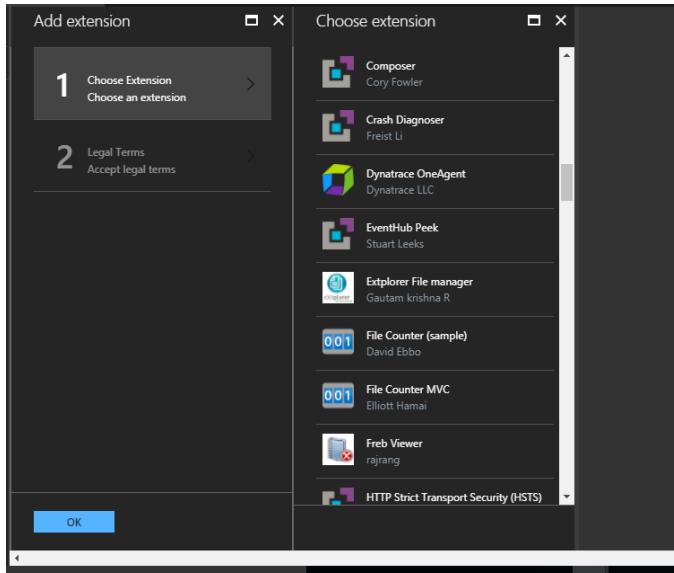
Install the Dynatrace Azure site extension

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

1. Open **portal.azure.com** in a new browser window.
2. Navigate to the web app you want to monitor.
3. Select **Extensions** from the list of options. You'll find this in the **Development tools** subsection (note the **Search** field at the top of the page in case you have trouble finding this option).
4. Within the new pane (i.e., "blade" in Azure terminology) that appears on the right-hand side, click **Add**.



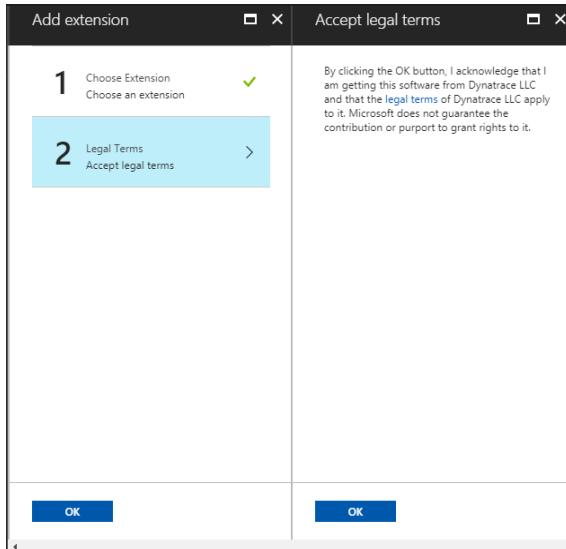
5. Scroll through the list until you find **Dynatrace OneAgent**. Note that entries are not ordered alphabetically. <https://help.dynatrace.com/images/content/infrastructure-monitoring/paas/extension.png>



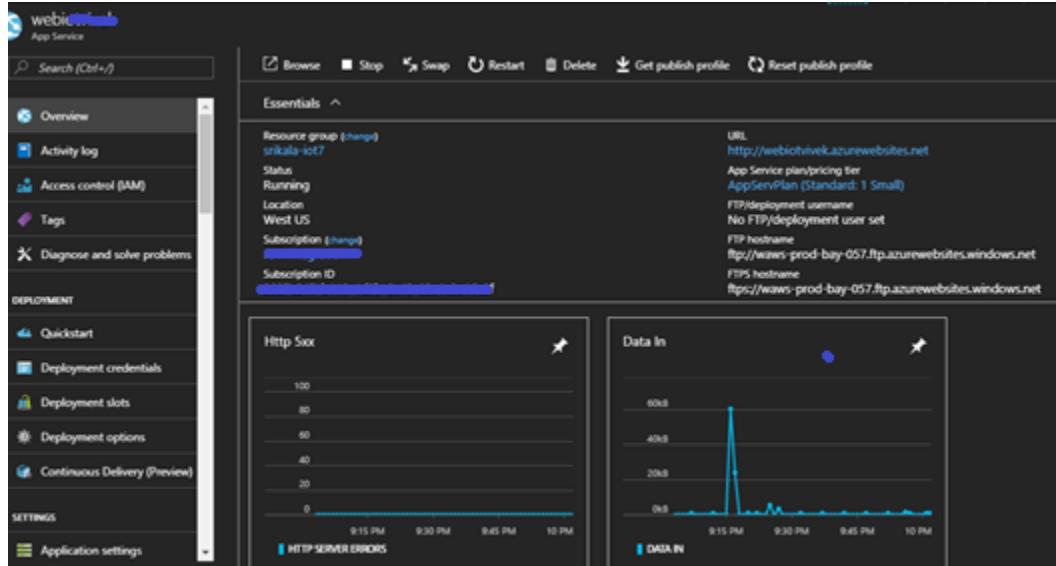
The screenshot shows the 'Extensions' blade in the Azure portal. The left sidebar includes 'Performance test', 'Resource explorer', 'Testing in production', and 'Extensions' (which is selected). Other sections like 'Easy tables', 'Easy APIs', 'Data connections', 'API definition', and 'CORS' are also listed. The main area shows a table with one item: 'Dynatrace OneAgent' (Version 1.15.121, Update Available: No). A note says: 'Extensions add functionality to your App Service. Click add to see the list of available extensions.'

NAME	VERSION	UPDATE AVAILABLE
Dynatrace OneAgent	1.15.121	No

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



- 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.



- 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: CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main area is titled "Services" and displays "All monitored services". It shows 2 services: "Running" and "Service type" "Webservice". The first service, "~iwebiotivek", has a response time of 571 ms, 0% failure rate, and 2 requests/min. The second service, "webiotivek", has a response time of 3.6 ms, 0% failure rate, and 1 request/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 Azure App Service Application settings page for the "webiotapp" application. The left sidebar lists settings: Application settings (selected), 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 is titled "Application settings" and contains a table of app settings. The table includes columns for Key, Value, Slot setting, and three-dot ellipsis. The settings listed are: restServer (https://apiserverw4j1.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 the table, there is a section for Connection strings 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 Slot setting.

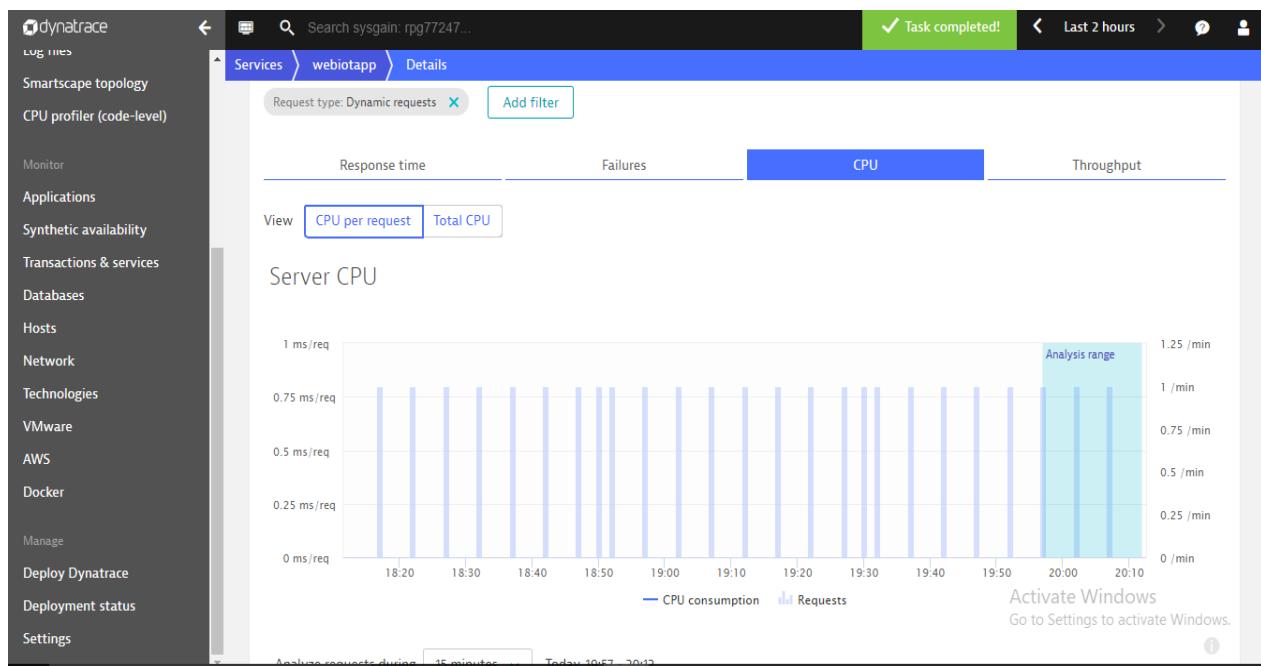
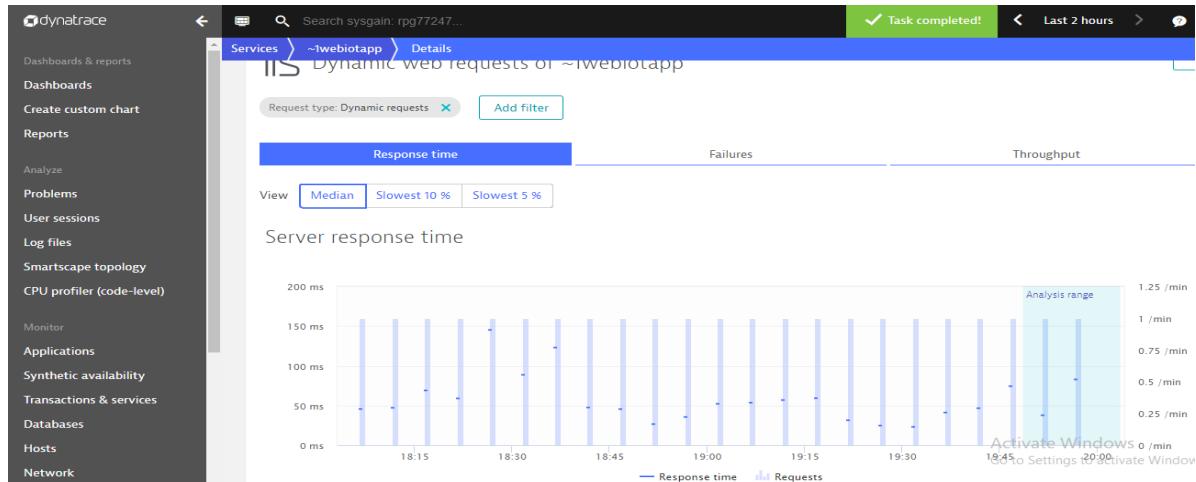
10. Once the application is restarted, navigate to the **Dynatrace Dashboard** and click on "**Transactions and Services**" to view the IOT application newly added.

The screenshot shows the Dynatrace Services dashboard. On the left, a sidebar lists various monitoring categories. The main area displays "All monitored services" with a count of 2. A table lists the services with their names, technologies, response times, failure rates, and throughput. The service "webiotapp" is listed under ASP.NET and IIS app pool, while the service "IIS ~1webiotapp" is listed under .NET and IIS app pool.

Name	Technology	Response time	Failure rate	Throughput
webiotapp	ASP.NET	0.89 ms	0 %	7 /min
IIS ~1webiotapp	.NET	59.6 ms	0 %	3 /min

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

The screenshot shows a detailed view of the IIS ~1webiotapp service. It includes a dependency diagram showing the flow from Application to Service through IIS App Pool, and another from Service to Database. Below this, there are three performance metrics: Response time (81.9 ms), Failure rate (0 %), and Throughput (1/min). To the right, sections for "Understand dependencies", "Analyze backtrace", and "Activate Windows" are visible.



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

The screenshot shows the Dynatrace application monitoring interface for the service 'webiotapp'. On the left, a sidebar lists various monitoring categories. The main area displays a service topology with nodes for Application, Service, ASP.NET, and Database, all showing 0 metrics. Below this is a section titled 'Dynamic web requests' with four metrics: Response time (1.83 ms), Failure rate (0 %), CPU (idle), and Throughput (1/min). A 'View dynamic requests' button is present. To the right, there's a summary stating 'No hotspots detected' and a 'Understand dependencies' section with a 'View service flow' button.

This screenshot shows the 'Service flow' details for the 'webiotapp' service. It starts with a summary for 'ASP .NET webiotapp' with an average response time of 77.9 ms and 26 requests. A 'View PurePaths' button is available. The main panel displays a 'Showing service flow of requests to 'webiotapp'' with a timeline for 'Today, 18:18 - 20:18 (2 Hours)'. A 'PurePath' visualization shows the flow of requests. A 'View PurePaths' button is also present here. Below this, a message says 'No service selected' with a note to select a service to get more details. A 'Activate Windows' message at the bottom encourages users to activate their Windows license.

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

The screenshot shows the Dynatrace web interface. On the left, there's a sidebar with a dark background containing links such as 'Log files', 'Smartscape topology', 'CPU profiler (code-level)', 'Monitor', 'Applications', 'Synthetic availability', 'Transactions & services', 'Databases', 'Hosts', 'Network', 'Technologies', 'VMware', 'AWS', 'Docker', 'Manage', 'Deploy Dynatrace', 'Deployment status', and 'Settings'. The main area has a light gray background. At the top, there's a navigation bar with 'Services > webiotapp > Details > Backtrace'. A green bar at the top right says 'Task completed!'. Below the navigation, it says 'Service-level backtrace of requests to 'webiotapp''. There's a date range selector 'Today, 18:20 - 20:20 (2 Hours)' with 'Apply' and 'Add filter' buttons. A descriptive text below the title explains that the service and applications listed make calls to this service, and the tree view represents the sequence of services and application user actions. The main content area is titled 'Incoming requests to this service' and shows a tree structure with 'ASP .NET IIS app pool webiotapp' expanded. To the right of the tree, there's a summary bar with a blue progress bar and the text '26 Requests' and '0 Failed requests'. In the bottom right corner of the main area, there's a message 'Activate Windows Go to Settings to activate Windows'.

7.2. Chef Automate

After the IOT arm template got successfully deployed, need to login to ChefAutomate and check the installed nodes status.

Step 1:

Login to the ChefWorkStation using below credentials.

Username: adminuser

Password: Password@1234

Note:

- To get the ChefWorkStation IP address, go to the Resource Group in the azure portal and click on "ChefWorkStation".
- Copy the IP address and open it "Remote Desktop Connection"

The screenshot shows the Azure portal interface for the 'chefworkstation' virtual machine within the 'srikala-iot8' resource group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, and Automation script. The main content area displays the 'Essentials' section with details like Subscription name (changed), IOT Integration, and Subscription ID. Below this is a table listing 66 items under 'VIRTUAL MACHINES', including 'chefworkstation' which is highlighted with a blue border. The table columns include NAME, TYPE, and LOCATION.

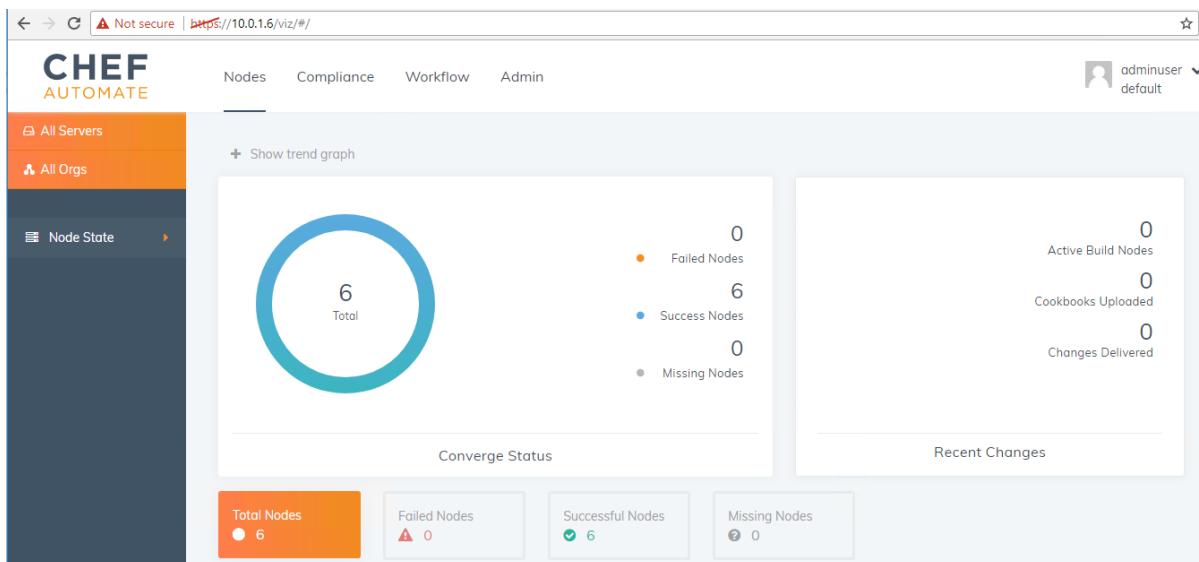
NAME	TYPE	LOCATION
adServer	Virtual machine	South Central US
baselineServer	Virtual machine	South Central US
chefautomate	Virtual machine	South Central US
chefworkstation	Virtual machine	South Central US
fortigate	Virtual machine	South Central US
PAASQlServer	Virtual machine	South Central US
PAASVMServer	Virtual machine	South Central US
sqlAnolisserver	Virtual machine	South Central US

This screenshot shows the detailed view of the 'chefworkstation' virtual machine. The left sidebar includes options for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Availability set, Disks, Extensions, Network interfaces, Size, Backup, and Properties. The main area displays the 'Essentials' section with resource group (changed), status (Running), location (South Central US), subscription (changed), IOT Integration, and subscription ID. A callout box highlights the 'Public IP address' field, which is 13.65.146.32. Below this, there are performance monitoring charts for CPU (average), Network (total), and Disk bytes (total).

Step 2:

Open ChefAutomate in browser using, IP address of ChefAutomate which you will get from the output section of IOT arm Template.

Under Nodes section, all the nodes which are added to Chef are listed.

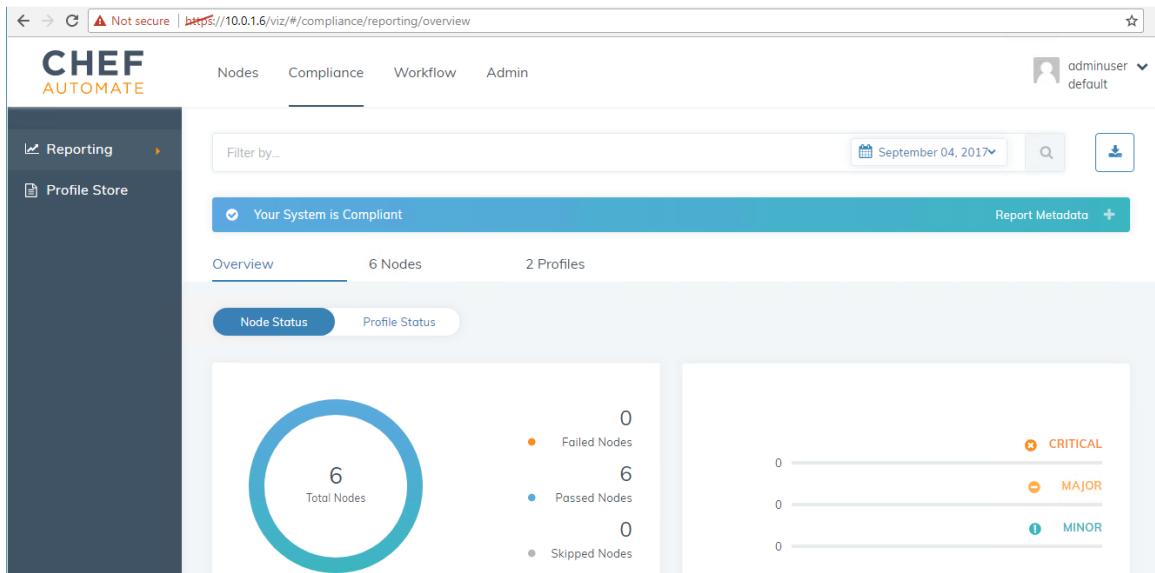


Converge	Node Name	Check-in	Uptime	Platform	Environment	
✓	adserver	3 days ago	an hour	windows	_default	>
✓	bastionserver	3 days ago	2 hours	windows	_default	>
✓	piafdasqlserver	3 days ago	an hour	windows	_default	>
✓	pibaserver	3 days ago	an hour	windows	_default	>
✓	trendserver	3 days ago	2 hours	centos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

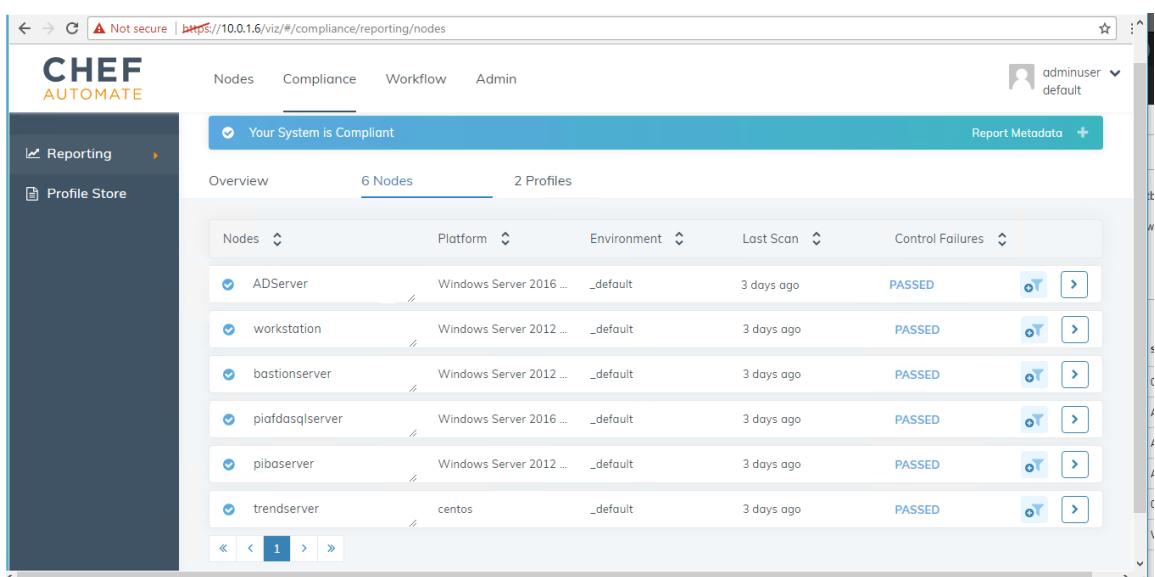
Step 3:

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

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



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



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

The screenshot shows the Chef Automate web interface under the 'Compliance' tab. A prominent message box at the top says 'This node is compliant. Great job!' with a checkmark icon. To the right, a summary box displays the last scan details: 'Last Scan' (September 1, 2017, 10:59 AM), 'Profiles' (1 Profiles), 'Platform' (Windows Server 2012 R2 Datacenter), and 'Environment' (_default). Below this, a grid of six status boxes shows: 'Total Controls' (32), 'Critical Controls' (0), 'Major Controls' (0), 'Minor Controls' (0), 'Skipped Controls' (0), and 'Passed Controls' (32). The main table below lists three compliance controls, all of which are critical (CRITICAL) and passed. Each row includes a '+' button to add the control to a profile.

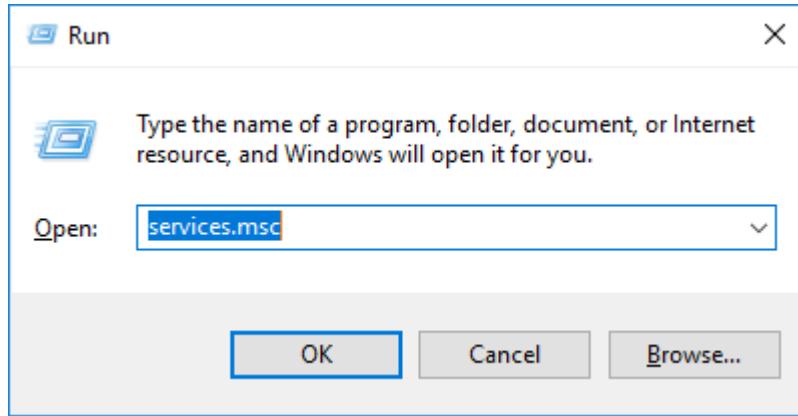
Control	Test Results	Severity	Root Profile
windows-base-100: Verify the Windows folder ...	1	CRITICAL (1)	windows-baseline
windows-base-101: Safe DLL Search Mode is E...	2	CRITICAL (1)	windows-baseline
windows-base-102: Anonymous Access to Win...	2	CRITICAL (1)	windows-baseline

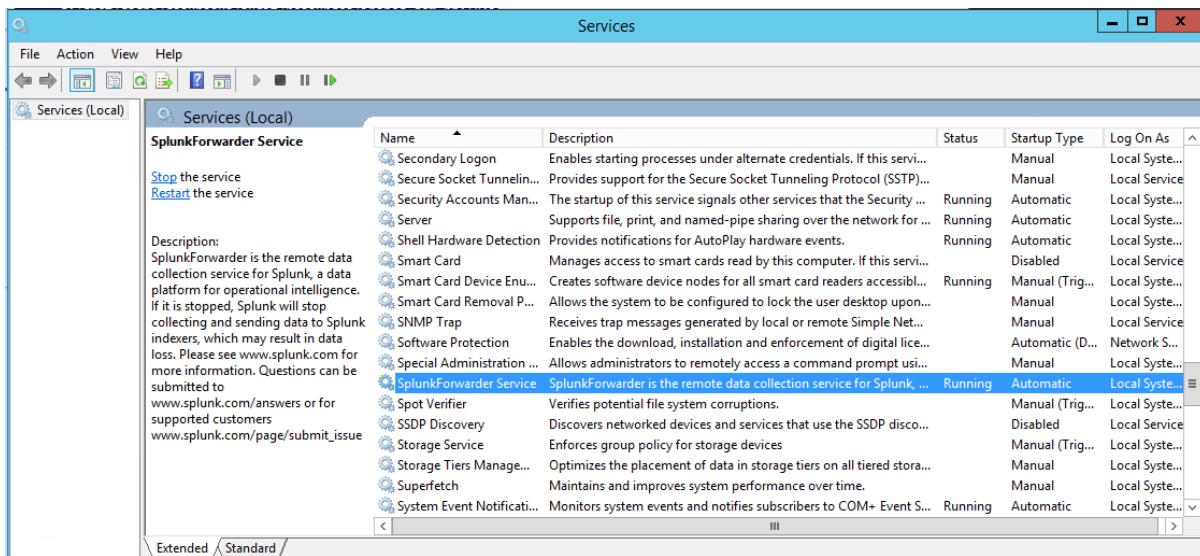
Splunk Universal Forwarder Installation Using Chef Automate:

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.

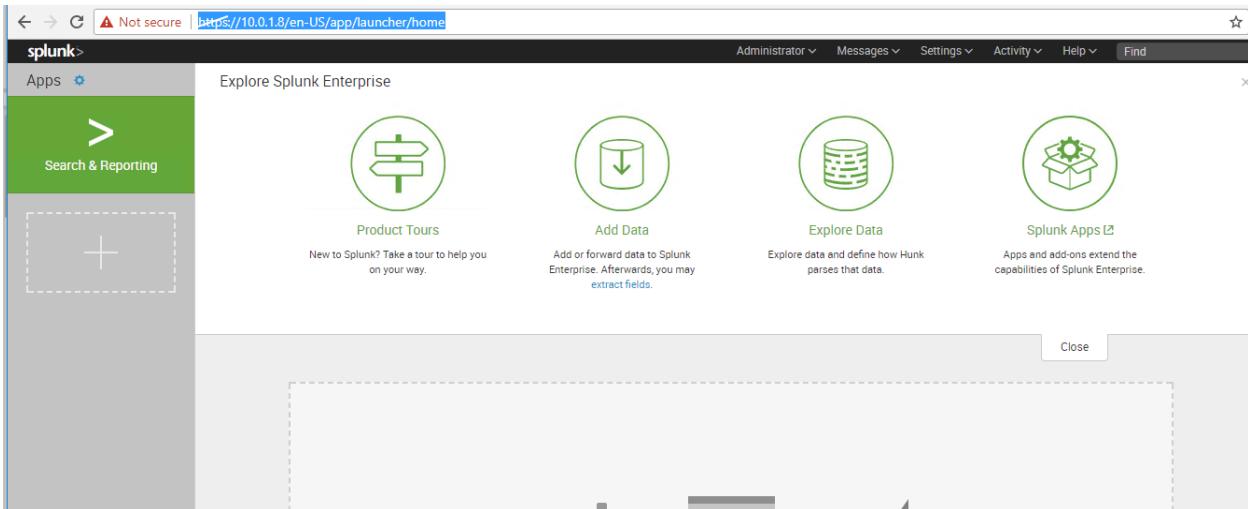
In our system Splunk server getting all windows logs from client machines automatically, for this we have installed splunk-forwarder using chef automate in every windows server. To view the logs in splunk server.

Step1:

Enter **https:10.0.1.8** in web browser and Login to the splunk server using below credentials

Username: admin

Password: Password@1234



Step2:

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

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

Step3:

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

The image contains two screenshots of the Splunk web interface. Both screenshots show the search bar at the top with the query `host="bastionserver"`. The first screenshot shows the search interface with various filters and summary statistics. The second screenshot shows the detailed event list with two log entries visible.

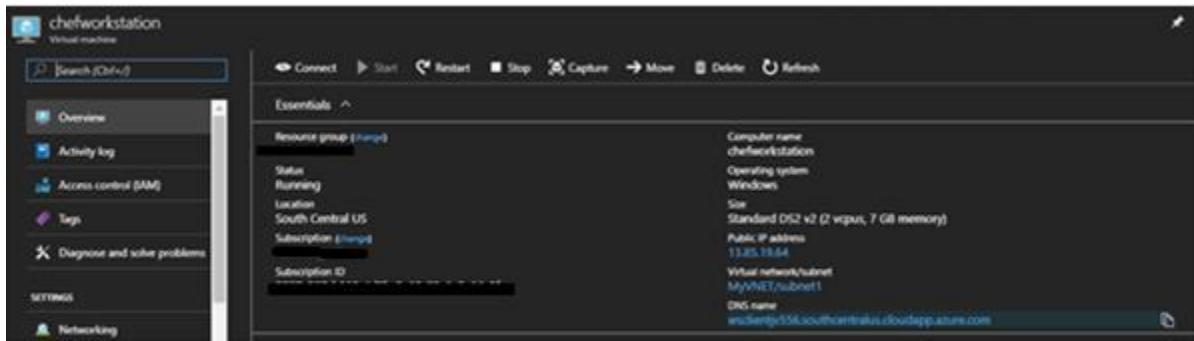
Time	Event
08/30/2017 12:21:25 PM	host = bastionServer source = WinEventLog:Security sourcetype = WinEventLog:Security
08/30/2017 12:21:04 PM	host = bastionServer source = WinEventLog:Security sourcetype = WinEventLog:Security

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

7.4. TrendMicro

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

Login to Bastion Host or ChefWorkstation server.

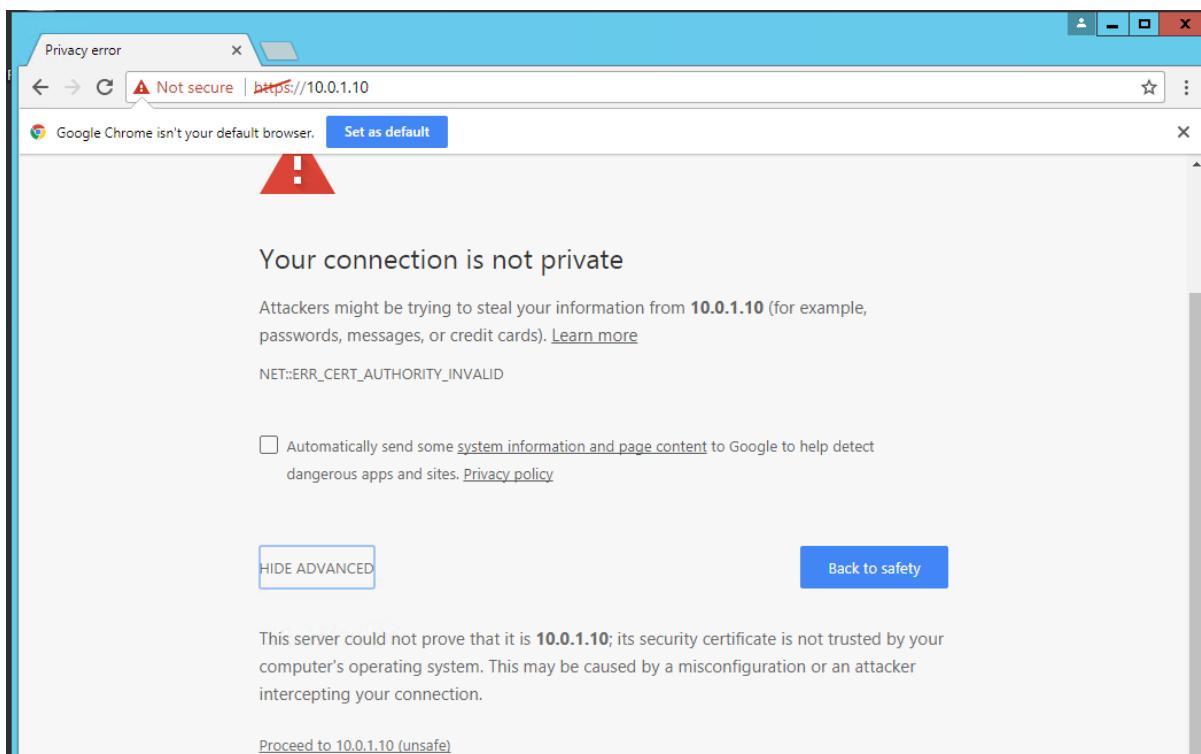
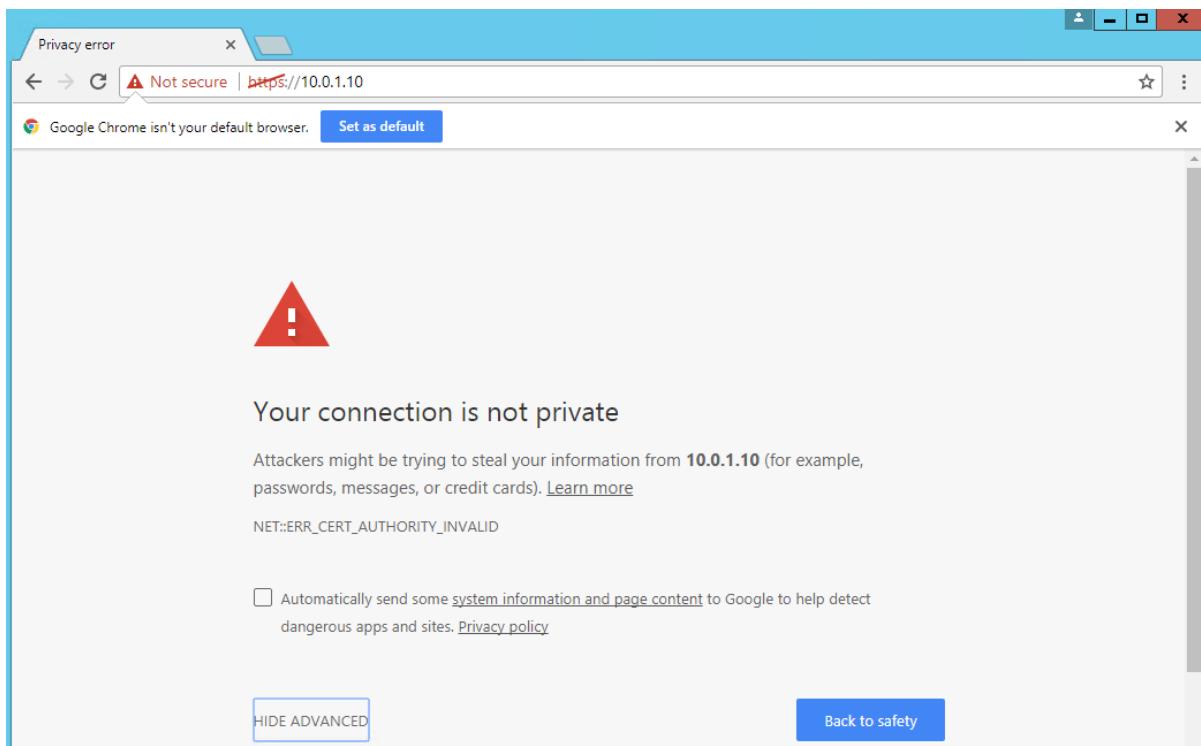


Once login open Browser and enter the TrendMicro IP address, which we get from output section of IOT ARM Template.

The screenshot shows the 'Microsoft.Template' deployment settings in the Azure portal. The left sidebar lists various resource types with icons. The main pane shows the following configuration parameters:

Parameter	Value	Action
WORKSTATIONFQDN	<code>wsclientjv556.southcentralus.cloudapp.azure.com</code>	
CHEFAUTOMATEIPADDRESS	<code>10.0.1.6</code>	
CHEFAUTOMATELOGINUSERNAME	<code>adminuser</code>	
TRENDIPADDRESS	<code>10.0.1.10</code>	
TRENDWEBUIUSERNAME	<code>adminuser</code>	
SPLUNKIPADDRESS	<code>10.0.1.8</code>	
SPLUNKWEBUIUSERNAME	<code>admin</code>	
FORTIGATEFQDN	<code>fortigatejv556</code>	
AZURESQLENDPOINT	<code>sqlserverjv556.database.windows.net</code>	
AZURESQLDBNAME	<code>azuredb</code>	
AZURESQLUSERNAME	<code>sqluser</code>	

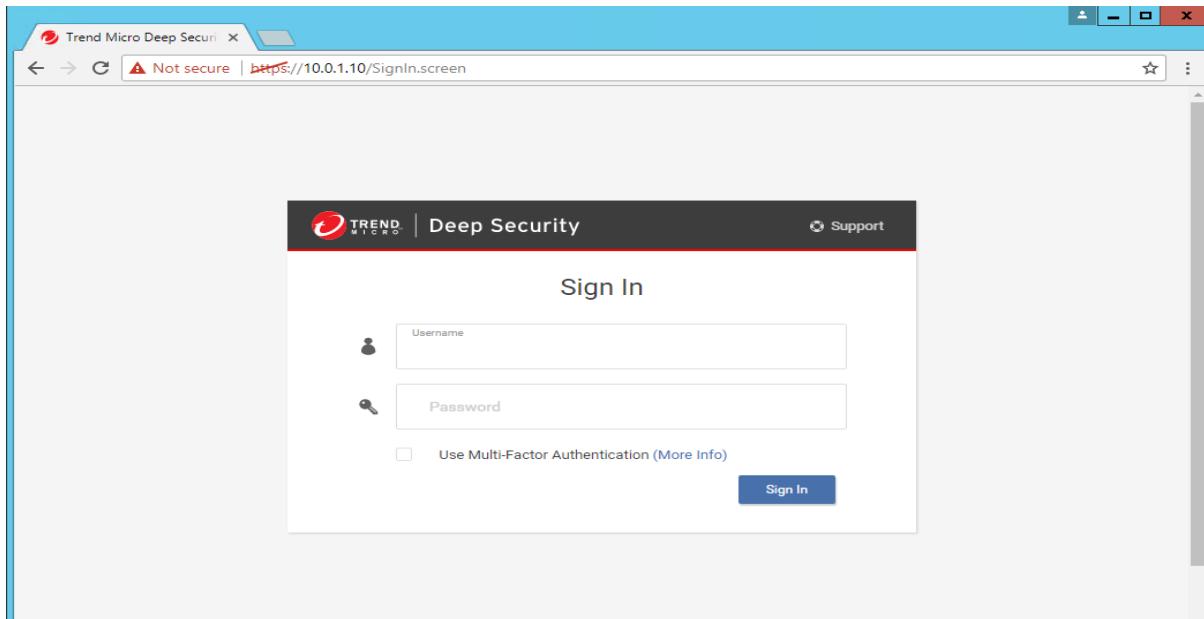
Click on "HIDE ADVANCED" and then click on "proceed to 10.0.1.10"



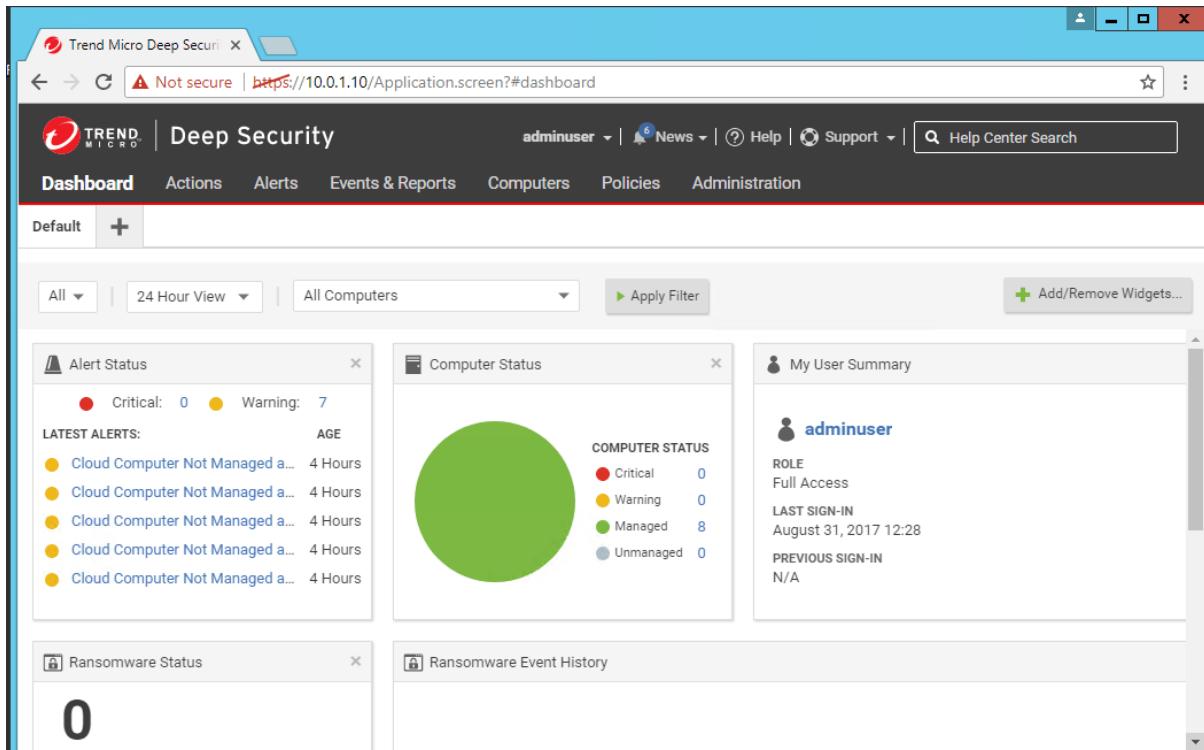
Login to Trend using the credentials.

Username: adminuser

Password: Password@1234



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

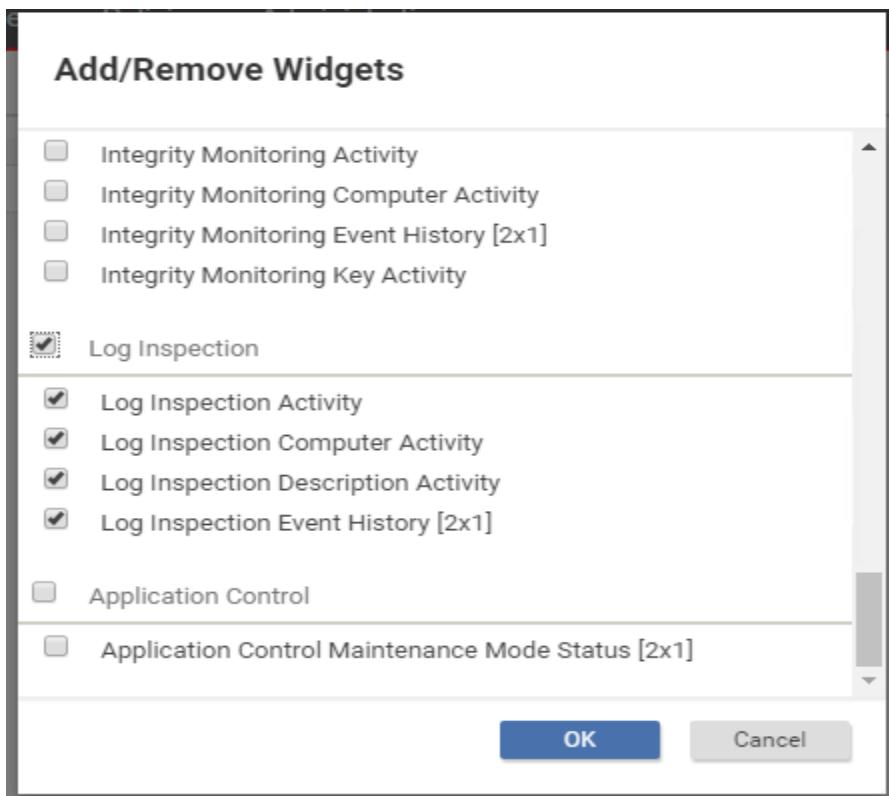


We can create our own Dashboard by clicking on "+" icon Besides Default and add the Widgets which you want to monitor.

The screenshot shows the Trend Micro Deep Security interface. At the top, there's a header bar with the Trend Micro logo and the text "Trend Micro Deep Securi". Below it, a navigation bar includes links for "Dashboard", "Actions", "Alerts", "Events & Reports", "Computers", "Policies", and "Administration". A user "adminuse" is logged in. In the main content area, there's a button labeled "Default" and a plus sign "+". A modal dialog box titled "Add New Dashboard" is open. It contains a text input field for "New Dashboard Name" with the value "Log Inspection" highlighted. There's also a checked checkbox for "Duplicate Current Dashboard". At the bottom of the dialog are "Add" and "Cancel" buttons.

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

The screenshot shows the "Log Inspection" dashboard configuration. At the top, a message says "Widgets are visible in this dashboard configuration. Use the Add/Remove Widgets... button to add widgets." Below this is a search bar with "Log Inspection" and a plus sign "+". Underneath are filters for "24 Hour View", "All Computers", and "Apply Filter". On the right side, there's a green "Add/Remove Widgets..." button.



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

The screenshot shows the main interface with a top navigation bar. The "Log Inspection" tab is selected. Below the navigation bar is a toolbar with filters: "All", "24 Hour View", "All Computers", and "Apply Filter". To the right of the toolbar is a "Add/Remove Widgets" button.

The main area displays three widgets:

- Log Inspection Computer Activity**: Subtitle: TOP 5 COMPUTERS FOR LOG INSPECTION EVENTS. Message: No Information Available.
- Log Inspection Activity**: Subtitle: TOP 5 REASONS FOR LOG INSPECTION EVENTS. Message: No Information Available.
- Log Inspection Event History**: Subtitle: EVENT SEVERITY. Message: Critical.

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

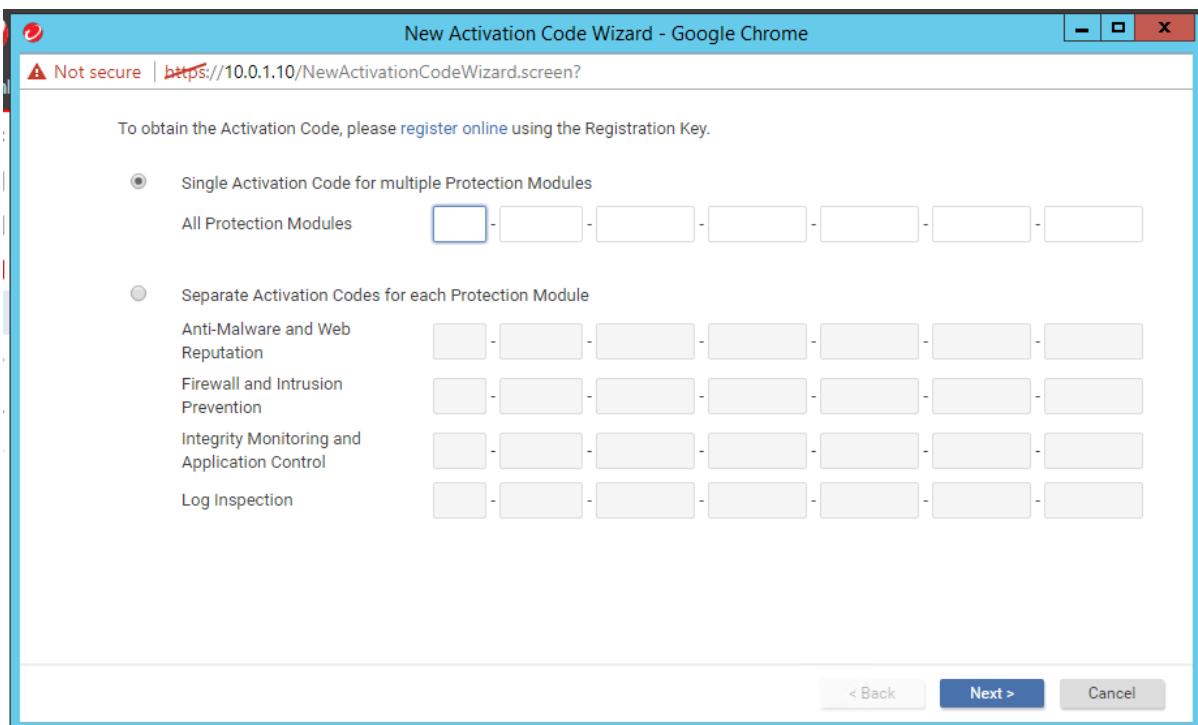
The screenshot shows the Trend Micro Deep Security web interface. The top navigation bar includes links for Dashboard, Actions, Alerts, Events & Reports, Computers (which is the active tab), Policies, and Administration. The left sidebar has sections for Smart Folders and Computers, with 'Computers' being the selected item. The main content area displays a table titled 'Computers' with columns for NAME, DESCRIPTION, PLATFORM, POLICY, STATUS, and MAINTENANCE. There are 8 entries listed, all of which are 'Managed (Online)' and have 'N/A' for maintenance. The table header also includes options for Add, Delete, Details, Actions, Events, Export, and Columns.

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 web interface with the 'Administration' tab selected. On the left sidebar, the 'Licenses' option is highlighted. The main content area is titled 'Licenses' and shows a table with a single row: 'License Mode: Bring your own license'. Below this, there is a table with four rows of data. Each row contains a protection module name, its status ('Not Licensed'), type ('N/A'), and expiration date ('N/A'). To the right of each row is a 'View Details...' button. At the bottom of the table, there is a text input field labeled 'Enter New Activation Code...'. The left sidebar also includes other administration options like System Settings, Scheduled Tasks, Event-Based Tasks, Manager Nodes, User Management, System Information, and Updates.

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



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

The screenshot shows the Trend Micro Deep Security Administration interface. The left sidebar has a "Licenses" section selected. The main content area is titled "Licenses" and shows the following information:

License Mode:		Bring your own license		
License Information last successful update on: September 4, 2017		Update Information		
	Status	Type	Expires	
Anti-Malware and Web Reputation	Activated	Full	September 28, 2017	View Details...
Firewall and Intrusion Prevention	Activated	Full	September 28, 2017	View Details...
Integrity Monitoring and Application Control	Activated	Full	September 28, 2017	View Details...
Log Inspection	Activated	Full	September 28, 2017	View Details...

At the bottom of the table, there is a button labeled "Enter New Activation Code...".

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

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

Click on Anti-Malware from left side menu.

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

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

Computer: 10.0.0.6

General Smart Protection Advanced Identified Files Anti-Malware Events

Anti-Malware

Configuration: Default (Off)

State: Off, not installed, no configuration

Real-Time Scan

Inherited

Malware Scan Configuration: No Configuration Edit

Schedule: Select Schedule Edit

Manual Scan

Inherited

Malware Scan Configuration: No Configuration Edit

Scheduled Scan

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

General Actions System Events

Hostname: 10.0.0.6 (Last IP Used: 10.0.0.6)

Display Name:

Description:

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

Group: Computers

Policy: None

Asset Importance: None

Download Security Updates From: Default Relay Group

Agent

Managed (Online)

Update of Configuration Pending (Heartbeat)

Task(s)

- Anti-Malware: On, Real Time
- Web Reputation: On, Real Time
- Firewall: On, Real Time
- Intrusion Prevention: On, Real Time
- Integrity Monitoring: On, Real Time

Save Close

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 Deep Security Administration interface. In the top navigation bar, there are links for Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, and Administration. The Administration tab is selected. On the left, a sidebar menu includes System Settings, Scheduled Tasks (which is currently selected and highlighted with a red box), Event-Based Tasks, Manager Nodes, Licenses, and User Management. Under User Management, there is a link for Users. The main content area is titled "Scheduled Tasks". It features a toolbar with buttons for New..., Delete..., Properties..., Duplicate, and Run Task Now. A search bar at the top right says "Search this page". Below the toolbar is a table with columns: NAME, TYPE, SCHEDULE, LAST RUN TIME, NEXT RUN TIME, ENABLED, and DETAILS. Two tasks are listed:

NAME	TYPE	SCHEDULE	LAST RUN TIME	NEXT RUN TIME	ENABLED	DETAILS
Daily check for Security Updates	Check for Security U...	Daily at 07:25 (UTC+0.00)	September 4, 201...	September 5, 201...	<input checked="" type="checkbox"/>	Check the Trend Micro Update
Daily check for Software Updates	Check for Software U...	Daily at 07:25 (UTC+0.00)	September 4, 201...	September 5, 201...	<input checked="" type="checkbox"/>	Check the Trend Micro Downl...

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. At the top, there are two tabs: "General" (selected) and "Task Details".

General Information

- Name:
- Type:
- Task Enabled:

Schedule Information

On the left, there is a list of scheduling options: Hourly, Daily (selected), Weekly, Monthly, Once Only.

Daily Schedule Details

- Start date: September 4, 2017
- Start time: 09:00
- Time zone: (UTC+0.00) Coordinated Universal Time (UTC)
- Frequency: Every Day (radio button selected)
- Weekdays:
- Every days

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

New Scheduled Task Wizard - Google Chrome

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

Select the computer(s) to update.

All Computers

In Group: Include sub-Groups

Using Policy: Include sub-Policies

Computer:

< Back **Next >** Cancel

Click on Finish

New Scheduled Task Wizard - Google Chrome

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

Enter a unique name for this scheduled task.

Name:

Type: Check for Security Updates

Schedule: Daily at 10:10 (UTC+0.00)

Next Run: September 4, 2017 10:10

Details: Computer: 10.0.0.6

Task Enabled

Run Task on 'Finish'

< Back **Finish** Cancel

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

The screenshot shows the Trend Micro Deep Security Administration interface. The left sidebar is titled 'Administration' and includes 'System Settings', 'Scheduled Tasks' (which is selected), 'Event-Based Tasks', 'Manager Nodes', 'Licenses', 'User Management' (with 'Users' and 'Roles' sub-options), and 'System Settings'. The main content area is titled 'Scheduled Tasks' and contains a table with columns: NAME, TYPE, SCHEDULE, LAST RUN TIME, and NEXT RUN TIME. There are three tasks listed:

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

At the top of the main content area are buttons for 'New...', 'Delete...', 'Properties...', 'Duplicate', and 'Run Task Now'.

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

The screenshot shows the Trend Micro Deep Security Administration interface. The left sidebar is identical to the previous screenshot. The main content area shows a message 'Running Task: Daily Check for Security Updates for chefWorkStation' in a green bar. Below it is the 'Scheduled Tasks' table, which now shows one task:

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

At the bottom of the screen, a progress bar indicates 'Performing Security Update on 1 Computer'.

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

The screenshot shows the Trend Micro Deep Security Computers interface. The left sidebar is titled 'Computers' and includes 'Smart Folders' and 'Computers' (which is selected). The main content area is titled 'Computers' and contains a table with columns: NAME, DESCRIPTION, PLATFORM, POLICY, STATUS, MAINTENAN..., and SEND POLICY SUCCESSFUL. There are two computer entries:

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENAN...	SEND POLICY SUCCESSFUL
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

At the top of the main content area are buttons for 'Add', 'Delete...', 'Details...', 'Actions', 'Events', 'Export', and 'Columns...'. A search bar is also present at the top right.

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

Computer: 10.0.0.6

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	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:59:59	Info	273	Security Update: Security Update Check and Download Requested	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	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	

Computer: 10.0.0.6

The screenshot shows the System Events section of a management interface. The left sidebar contains various monitoring categories like Anti-Malware, Web Reputation, Firewall, etc. The main area displays a list of events with columns for TIME, LEVEL, EVENT ID, and EVENT. A context menu is open over the second event in the list, showing options like 'Select All (14)', 'Export Selected to CSV...', 'View', 'Add Tag(s)...', and 'Remove Tag(s)...'. The events listed include security updates for pattern updates and security check requests.

TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...	TAR
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	273	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:25:12	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:20:25	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:15:12	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:15:12	Info	273	Events Retrieved	Agent	10.0	
September 4, 2017 08:15:12	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	

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

The screenshot shows a file explorer window titled 'Trend Event logs'. It lists two files: 'System_Events (1)' and 'System_Events'. Both files are Microsoft Excel files from 04-09-2017 at 14:36, each 1 KB in size.

The screenshot shows an Excel spreadsheet with the following data:

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

The screenshot shows an Excel spreadsheet with the following data:

	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.

The screenshot shows the Trend Micro Deep Security Manager interface. At the top, there's a navigation bar with links for Dashboard, Actions, **Alerts**, Events & Reports, Computers, Policies, and Administration. Below the navigation bar, there are two alert cards:

- Recommendations have been made for 1 Computer(s)**: This alert was generated 1 Hour Ago. It states that the security configuration of one computer needs updating. The computer listed is 10.0.0.5. There are buttons to Hide Details, Dismiss Selected, or Dismiss All.
- Licensing for Anti-Malware and Web Reputation Expires (September 28, 2017)**: This alert was generated August 31, 2017 at 12:43. It informs the user that their protection module license will expire soon and provides a link to change the license on the Administration > Licenses page.

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

The screenshot shows the Trend Micro Deep Security Manager interface with the Alerts tab selected. The page includes a search bar for filtering by Severity (e.g., Equals, Warning) and a toolbar with View, Dismiss, and Configure Alerts buttons. A table lists the alerts:

TIME	SEVERI...	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	

At the bottom right, there's a summary box labeled "ALERTS" with the numbers "12" and "0".

USES:

1. Adding computer to deep security manager

Use the computers page of the deep security manager to discover local computers or to connect to your cloud

2. Deploying protection

Deep security Agents are available for a wide variety of platforms. You can install the Agents manually or take advantage of the automation tools available for cloud provider such as deployment scripts for VM Extension for Microsoft Azure.

3. Assigning security policies

Next, assign security policies based on the types of systems you're protecting. Deep Security comes with a collection of policies designed for a variety of platforms and purposes - you can use these policies or create your own.

4. Keeping your protection up to date

The Trend Micro Smart Protection network updates the protection modules on your computers as soon as new threats are identified.

5. Keeping informed of Deep security events

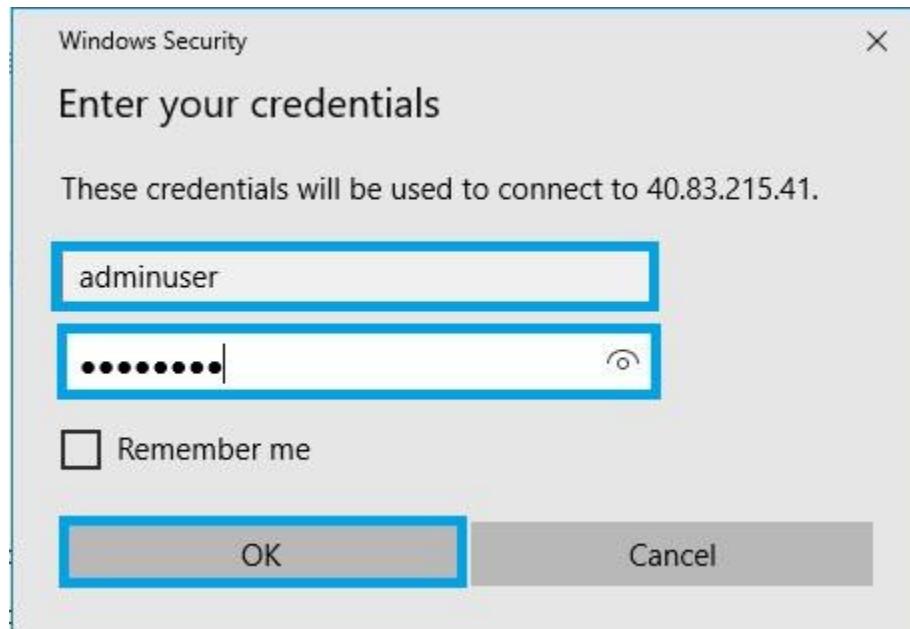
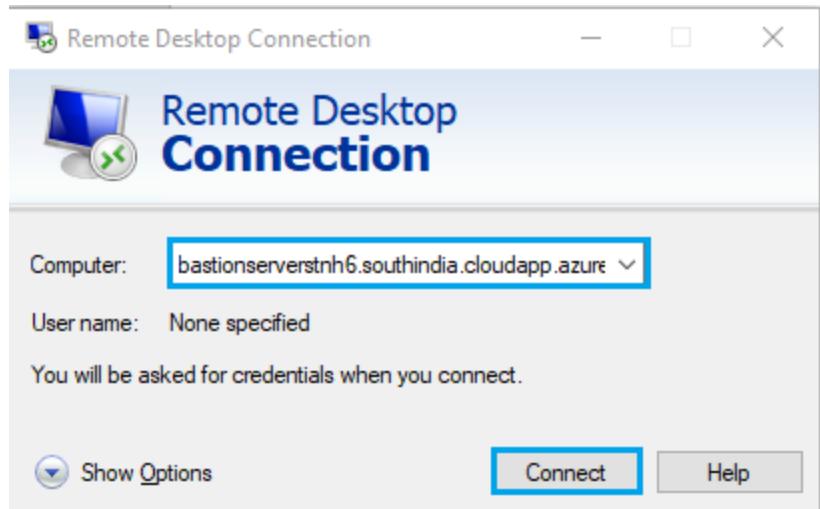
Use the customizable dashboard for quick, at-a-glance, views of the status of your Deep security system. Create scheduled Tasks to periodically send out customizable reports and set up your user account to receive notifications by email of important alerts

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

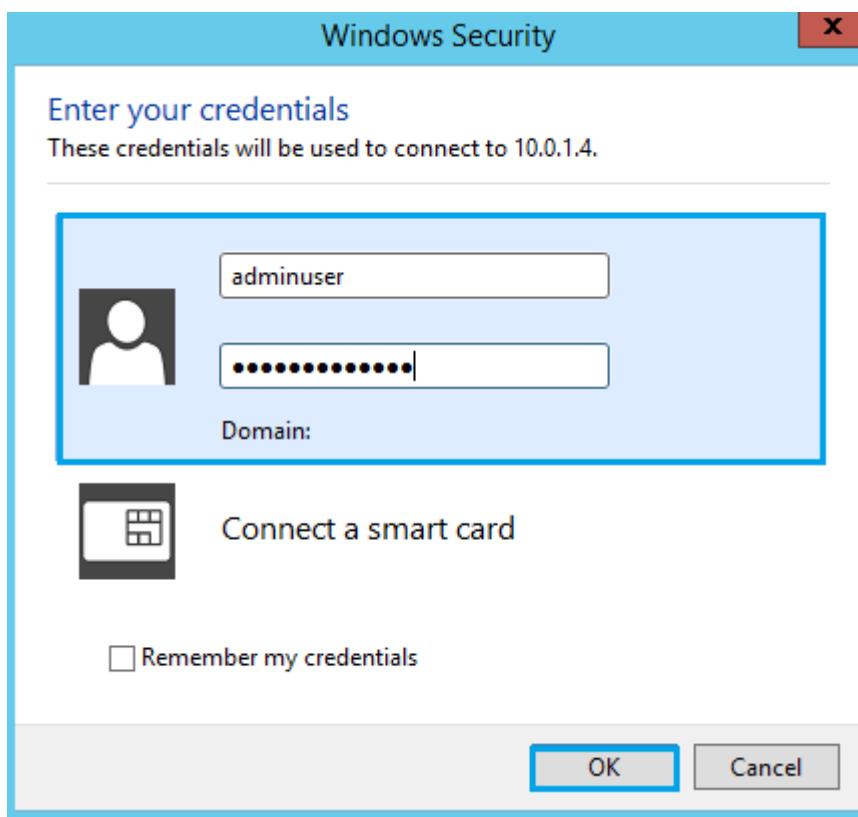
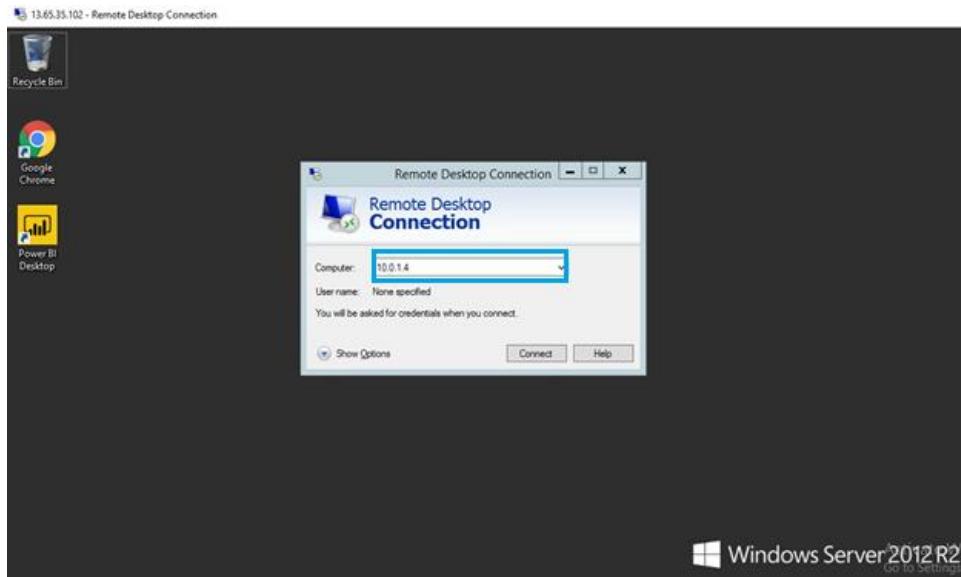
1. Login to the **Bastion Host VM** using **BASTIONFQDN** and **ADMINUSERNAME** provided in the **Outputs** section

Outputs

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



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



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



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

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
Saved Queries
sysgainiot.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users

Name	Type
bastionServer	Computer
chefworkstation	Computer
PIAFSQLServer	Computer
PIBAVMServer	Computer

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane lists 'Active Directory Users and Com', 'Saved Queries', and a expanded 'sysgainiot.com' node containing 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Accour', and 'Users'. The 'Computers' folder is highlighted with a blue selection box. On the right, a table displays four computer objects: 'bastionServer', 'chefworkstation', 'PIAFSQLServer', and 'PIBAVMServer', all categorized as 'Computer' type.

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

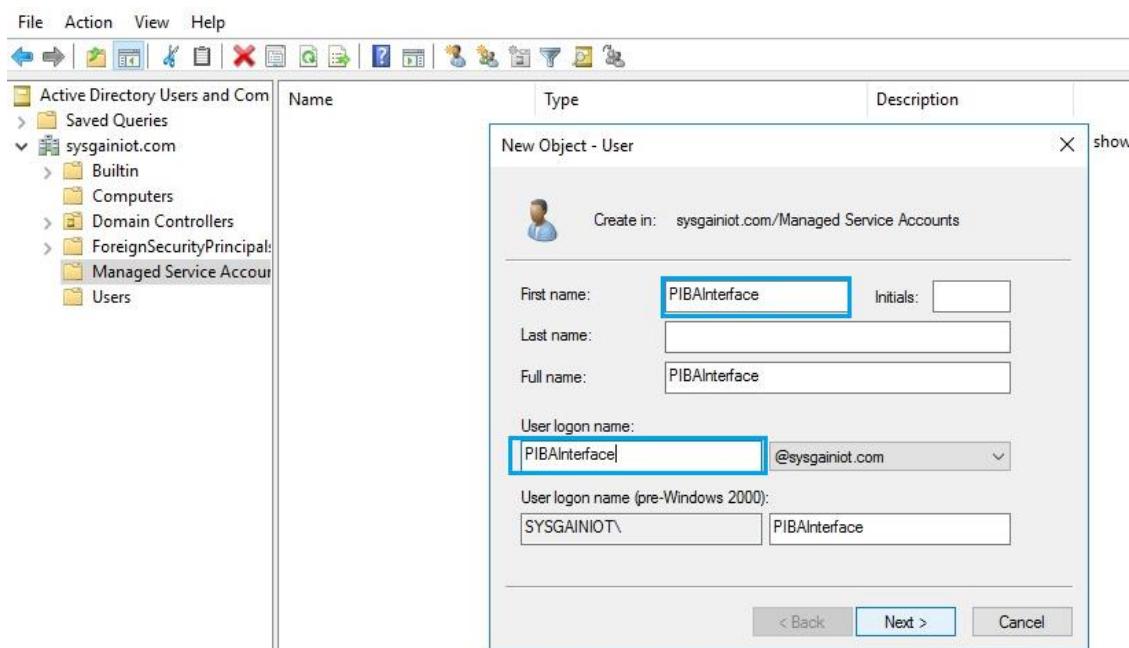
File Action View Help

Active Directory Users and Com
Saved Queries
sysgainiot.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service A...
Users

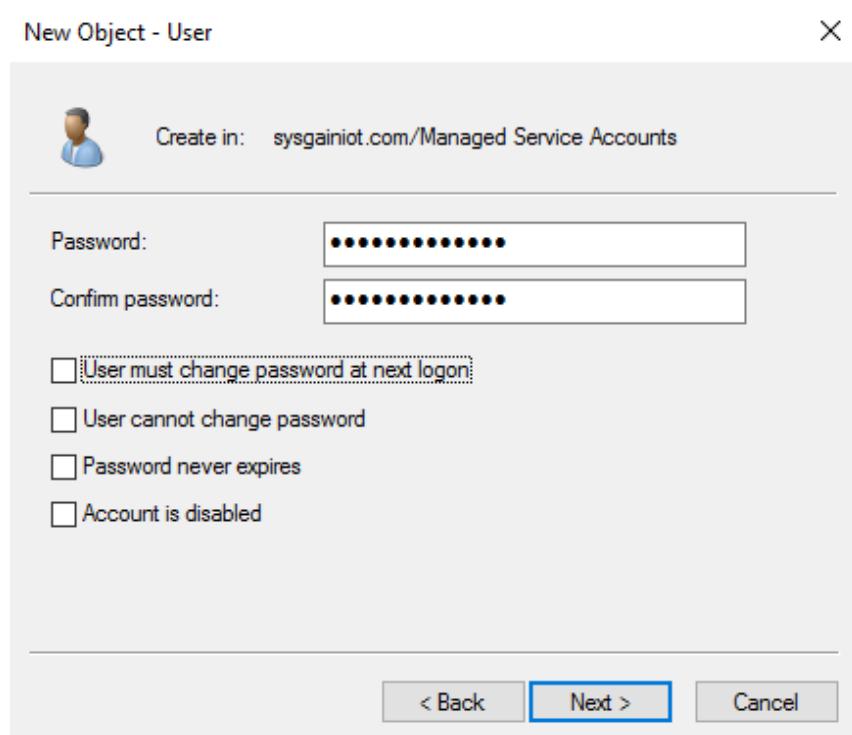
New Computer
All Tasks Contact
View Group
Cut InetOrgPerson
Delete msDS-KeyCredential
Rename msDS-ResourcePropertyList
Refresh msDS-ShadowPrincipalContainer
Export List... msImaging-PSPs
Properties MSMQ Queue Alias
Help Printer
User Shared Folder

The screenshot shows the same Active Directory interface as the previous one, but with a context menu open over the 'Managed Service A...' folder. The 'New' option is highlighted with a blue selection box. A secondary menu is displayed below it, listing various object types: Computer, Contact, Group, InetOrgPerson, msDS-KeyCredential, msDS-ResourcePropertyList, msDS-ShadowPrincipalContainer, msImaging-PSPs, MSMQ Queue Alias, Printer, User, and Shared Folder.

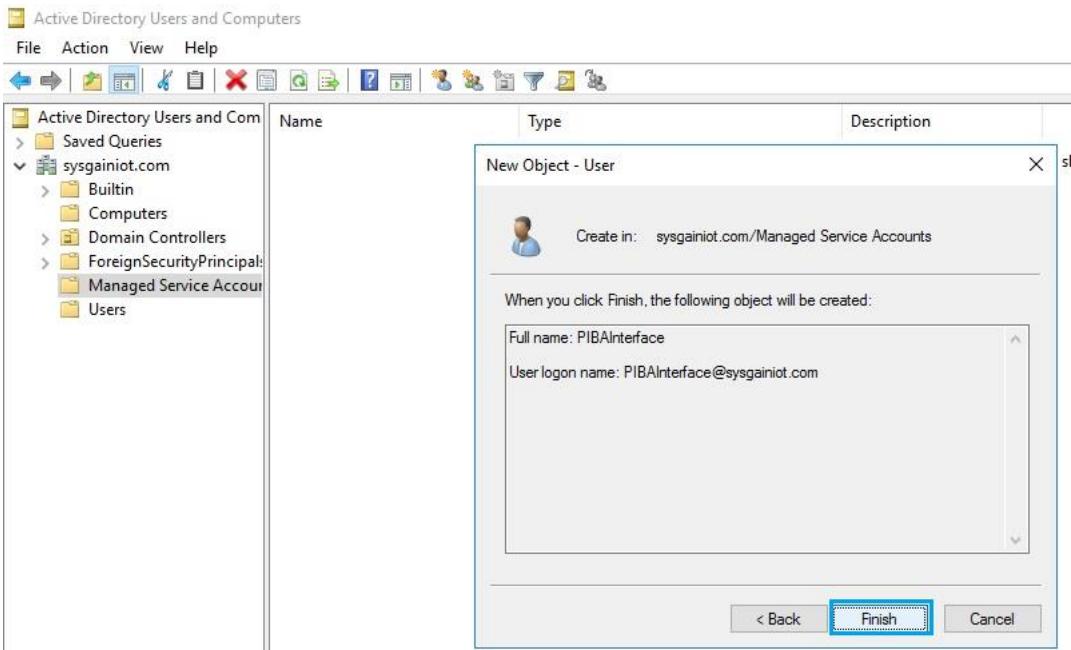
6. To create the user for PIBA, enter the **First name** and **User logon name**. Make sure both are the same. Click on **Next**.



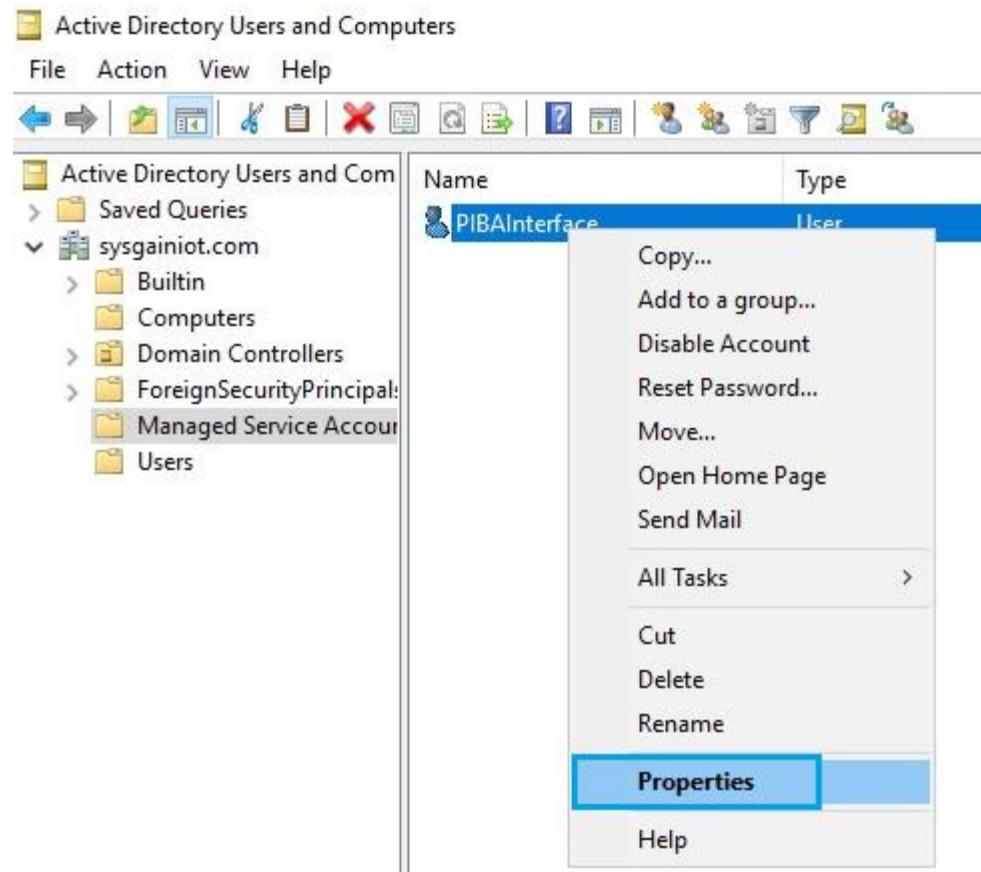
7. Enter the **Password** and uncheck **User must change password at next logon**. Click on **Next**.



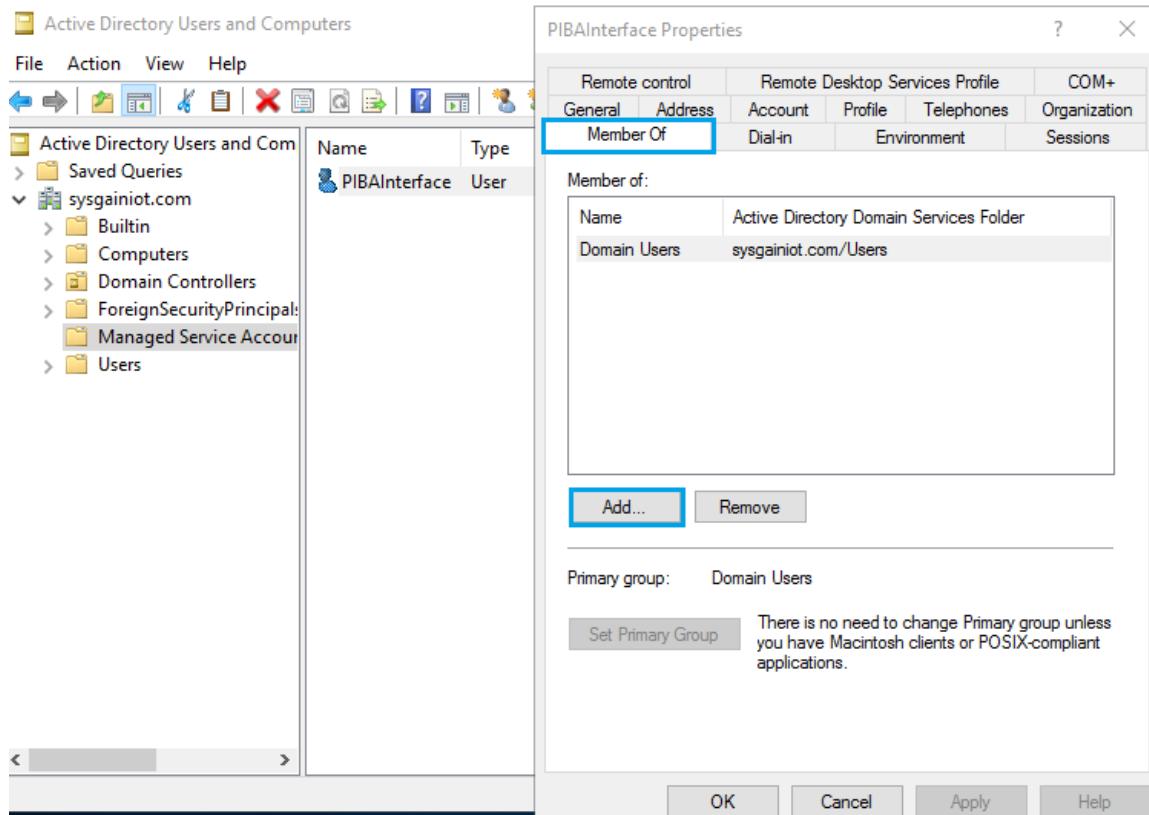
8. Click **Finish** once the object is created.



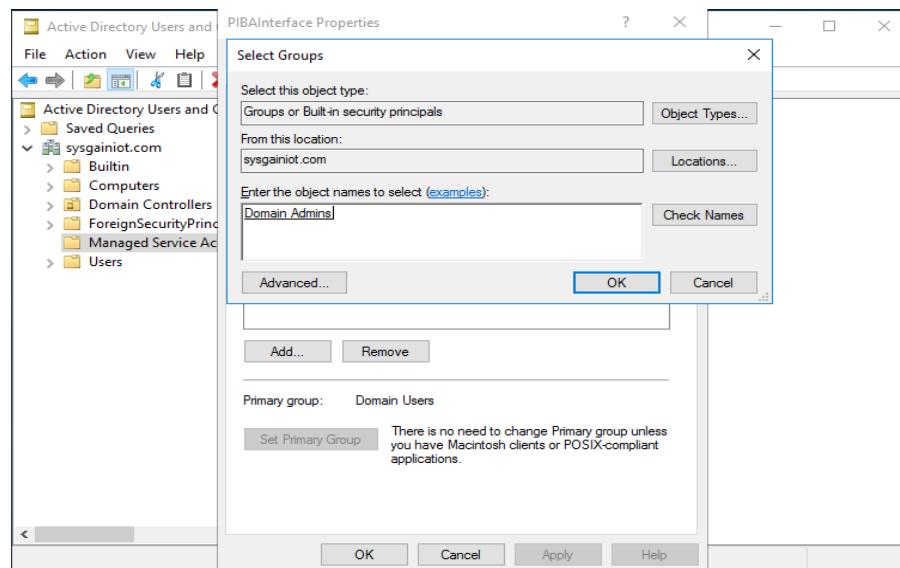
9. Check on the properties of the user created. Right click on the **PIBAInterface** and click on **Properties**.



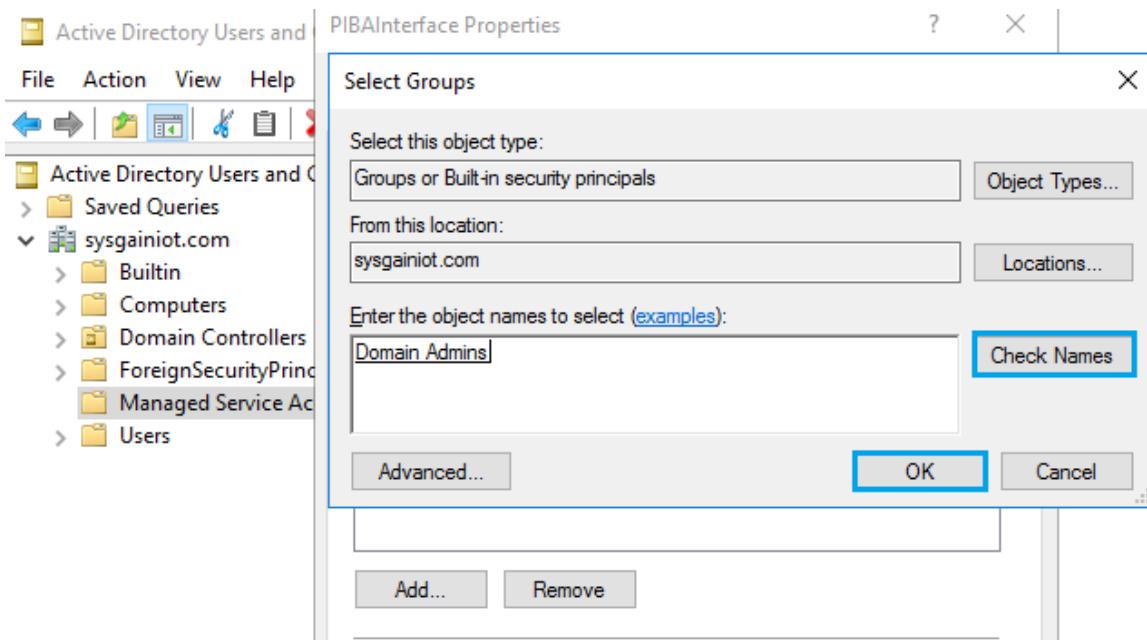
10. A popup will appear. Click on the **Member Of** tab and click the **Add** button.



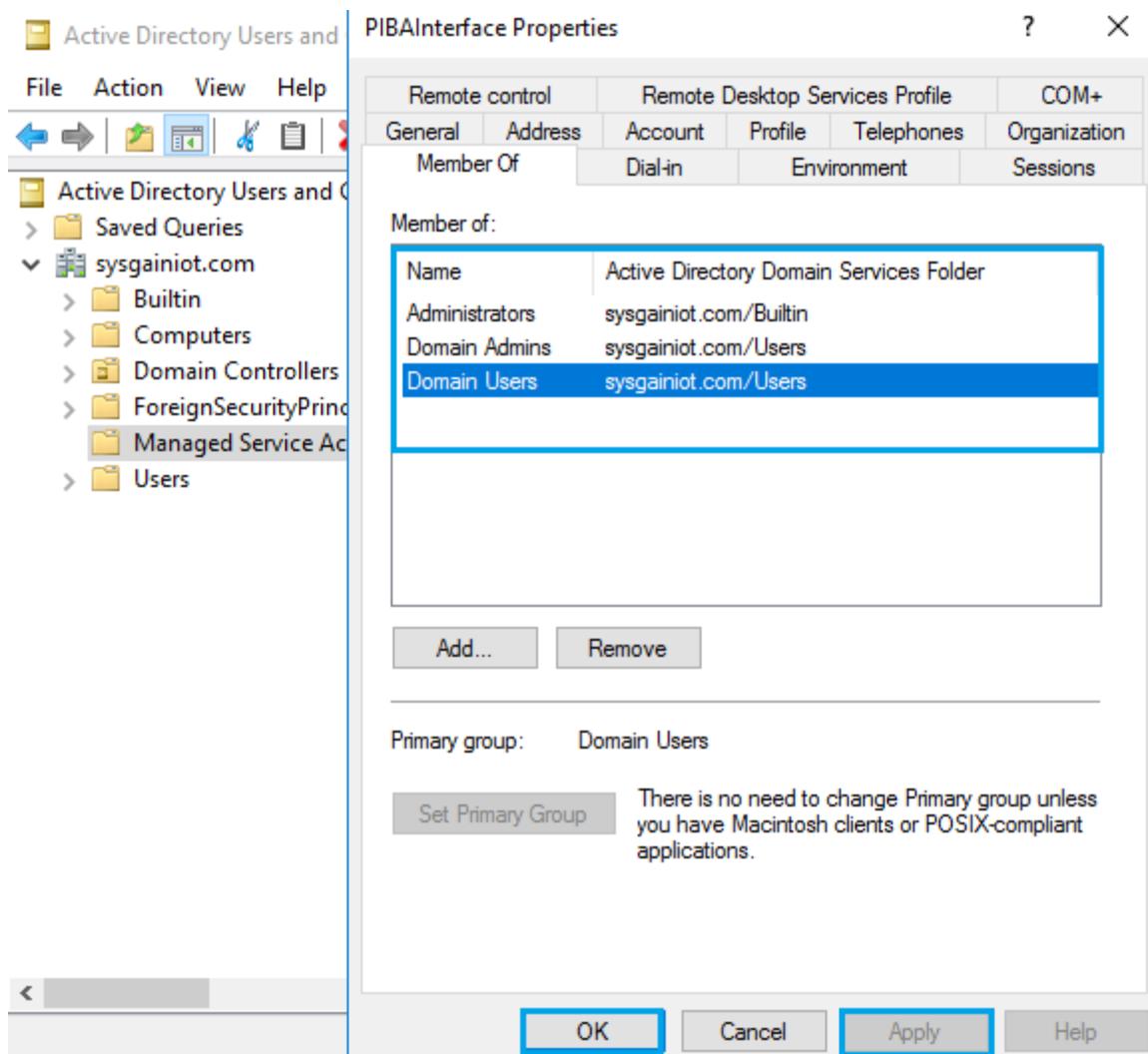
11. Enter the object name as **Domain Admins** and click on **Check Names**. It will display the Domain Admins as object names. Click on **Ok**. After that, click on **Ok** again. You will see the Domain Admin name added to the **Member of** section.



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

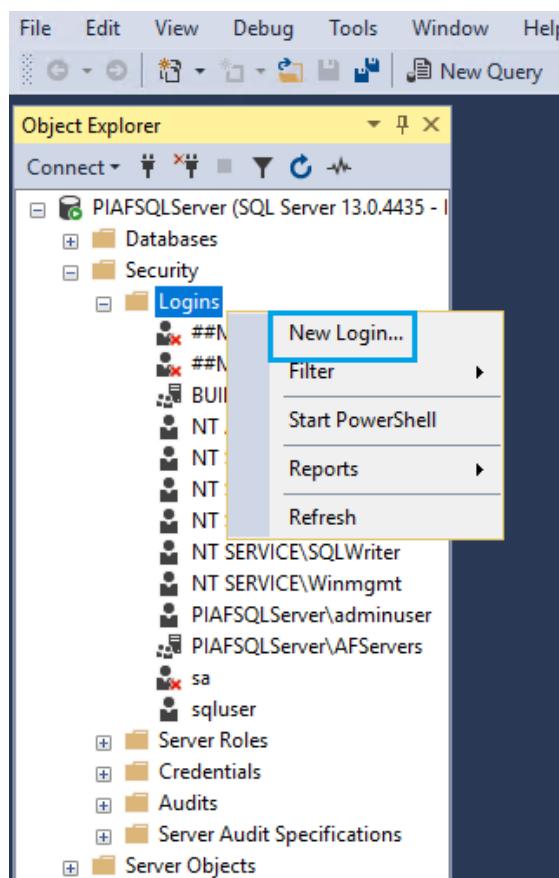
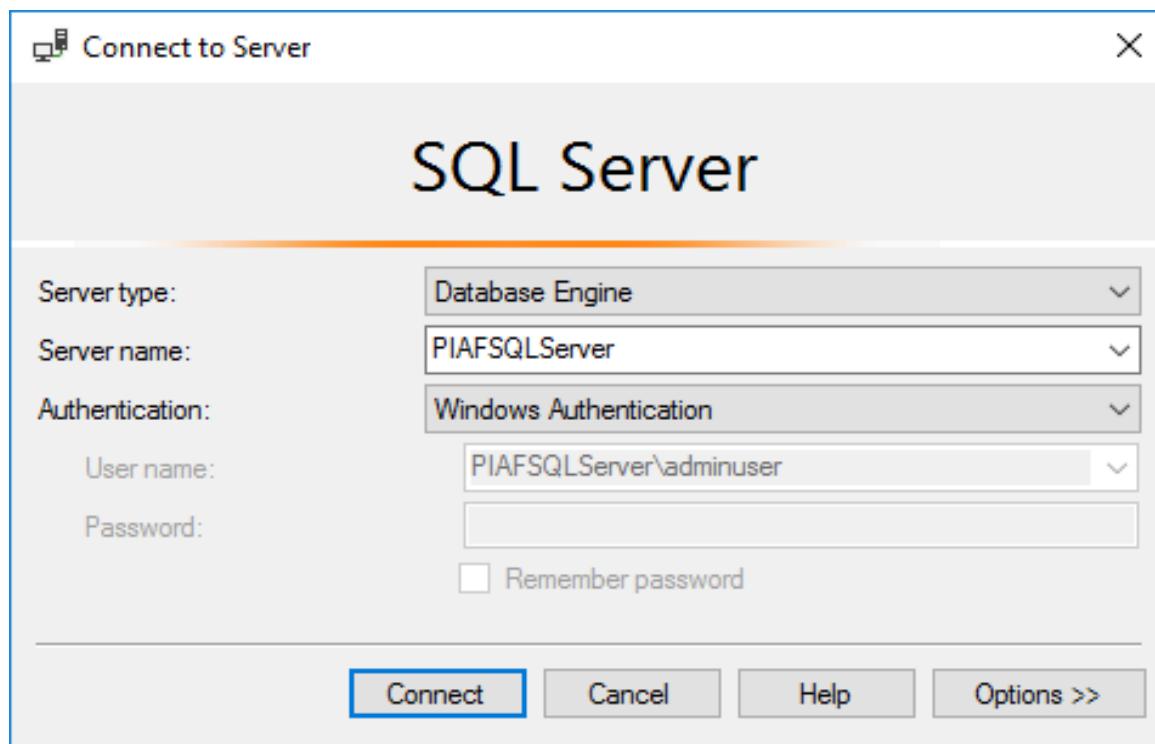
1. From the Bastion host, connect to the **PIAF** through the private IP address with the credentials provided in the output section.

Outputs

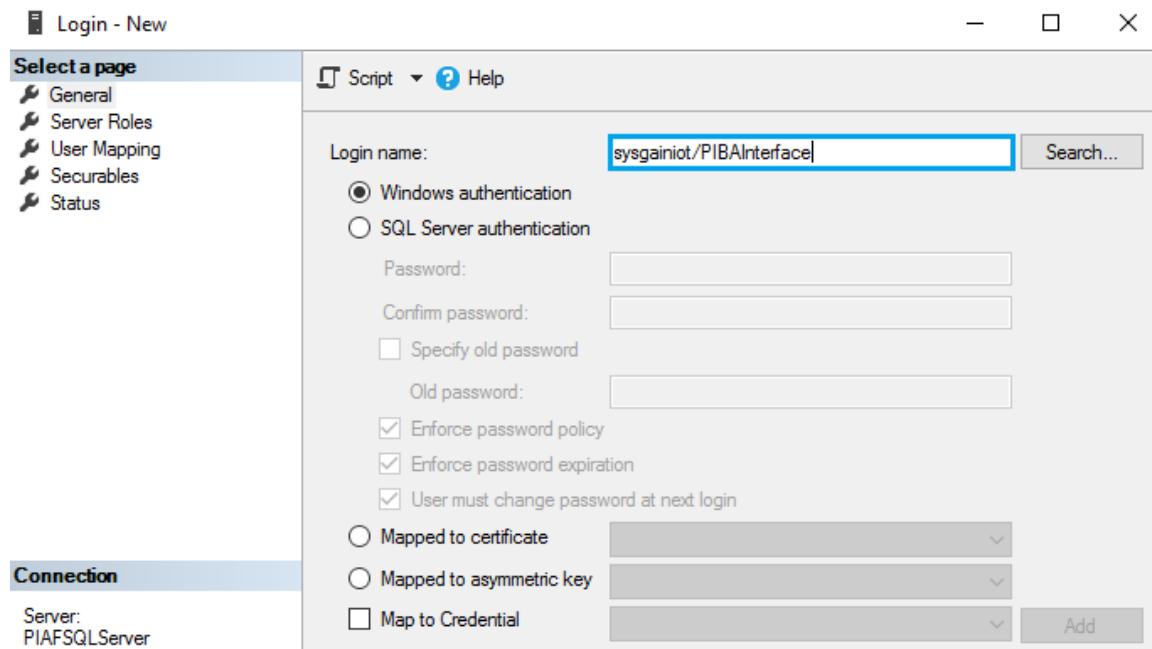
ADMINUSERNAME	adminuser	
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com	
ADSERVERIPADDRESS	10.0.1.4	
PIAFSQLSERVERIPADDRESS	10.0.2.4	



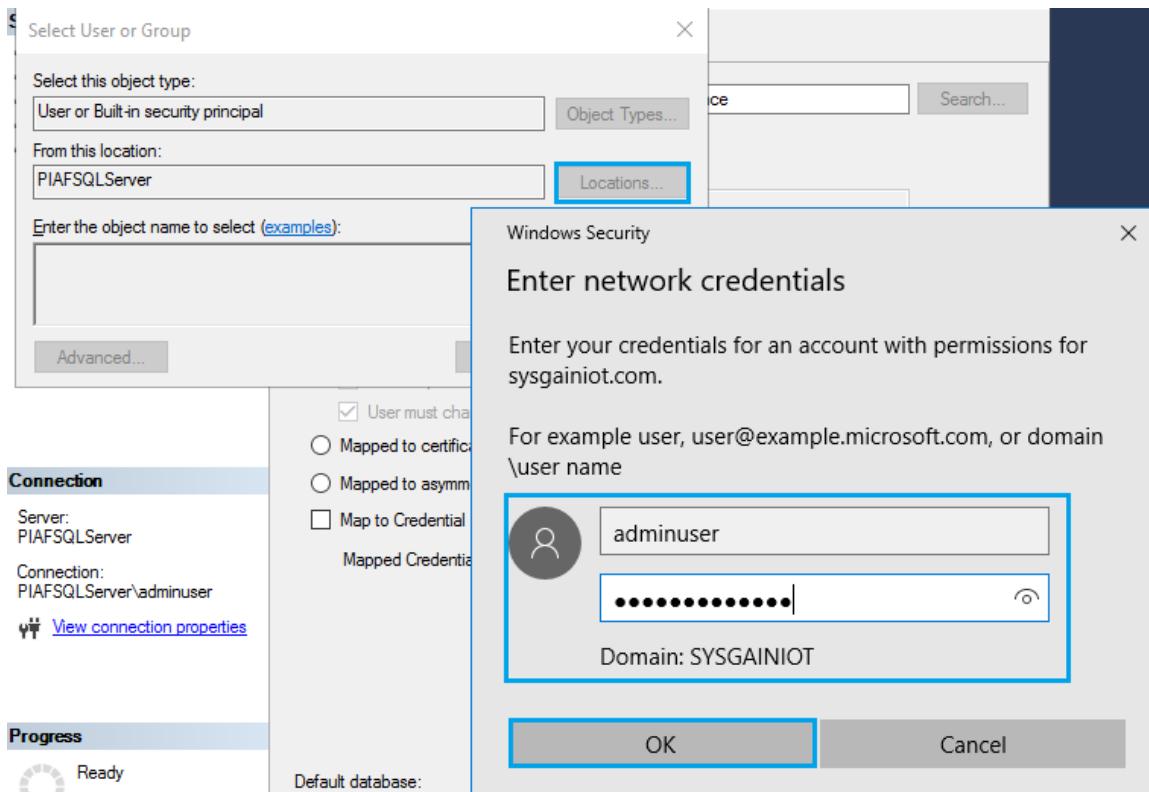
2. After logging in to the PIAF SQL Server, search for **ssms** in start menu to open the open the **SQL Server Management Studio** and create a new login by navigating to **Security** > Right-click on **Logins** and selecting **New Login**.



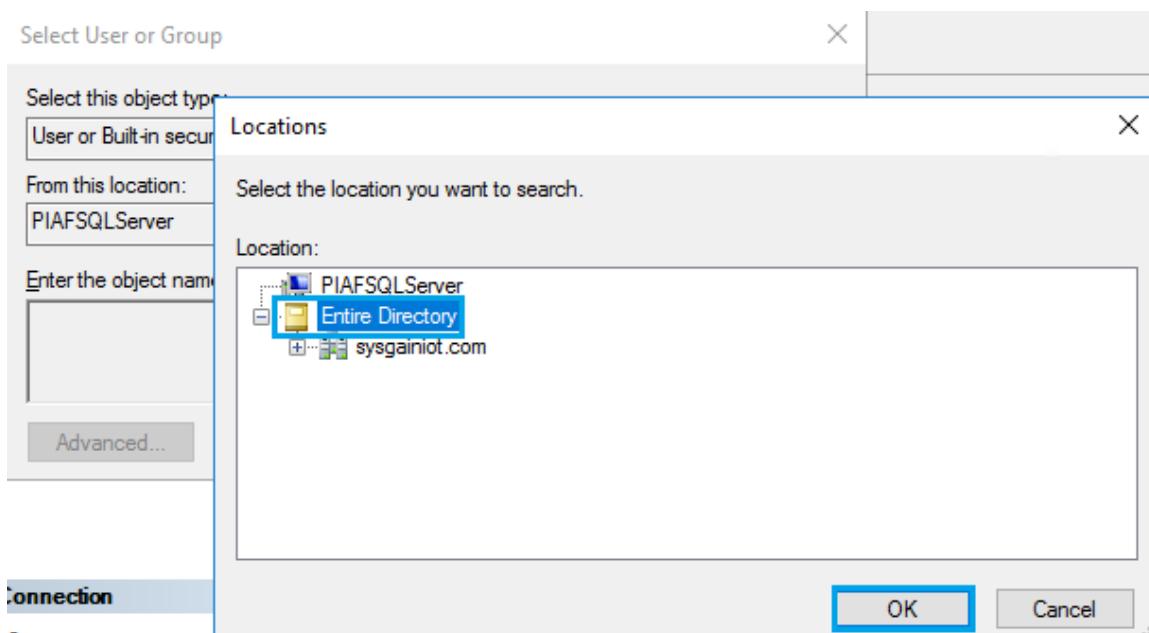
3. Give the login name as <domain name>/PIBAInterface, then click on **Search**.



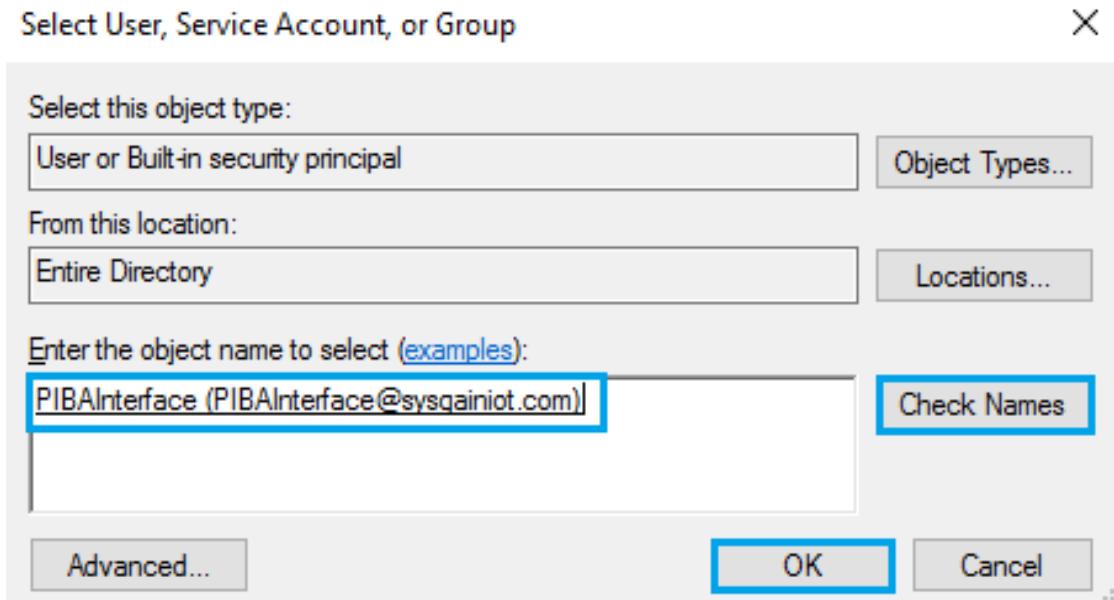
4. Click on **Locations**. You will get a popup box of credentials: enter the SQL server credentials.



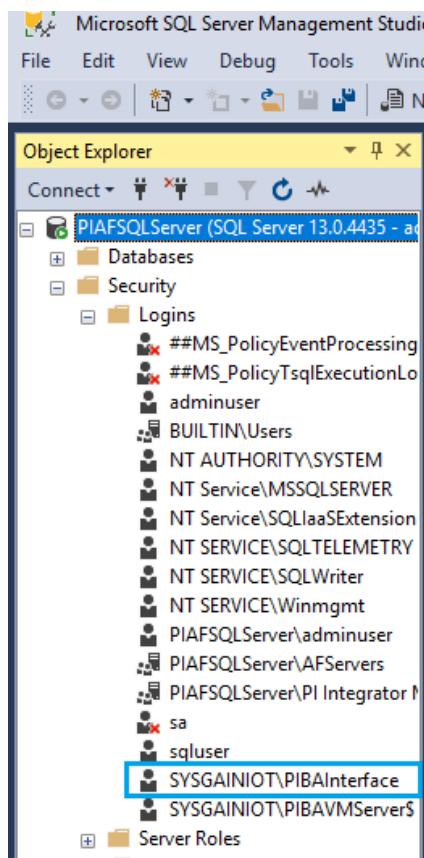
5. Select the **Entire Directory** and click on **OK**.



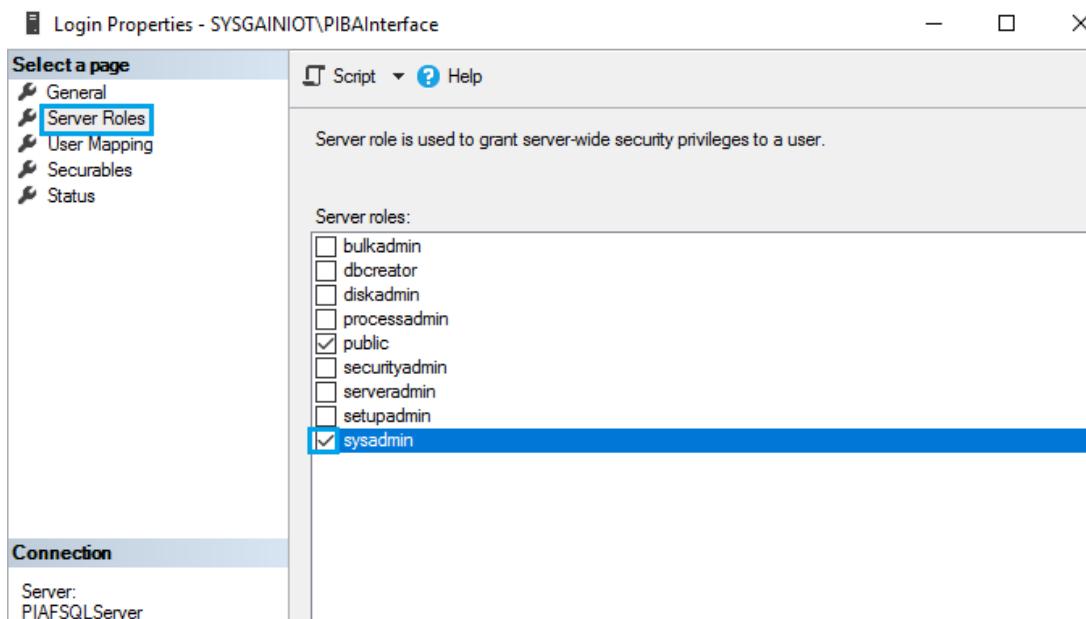
6. Enter the object name as **PIBAInterface** and click on **Check Names**. Then click on **OK**



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

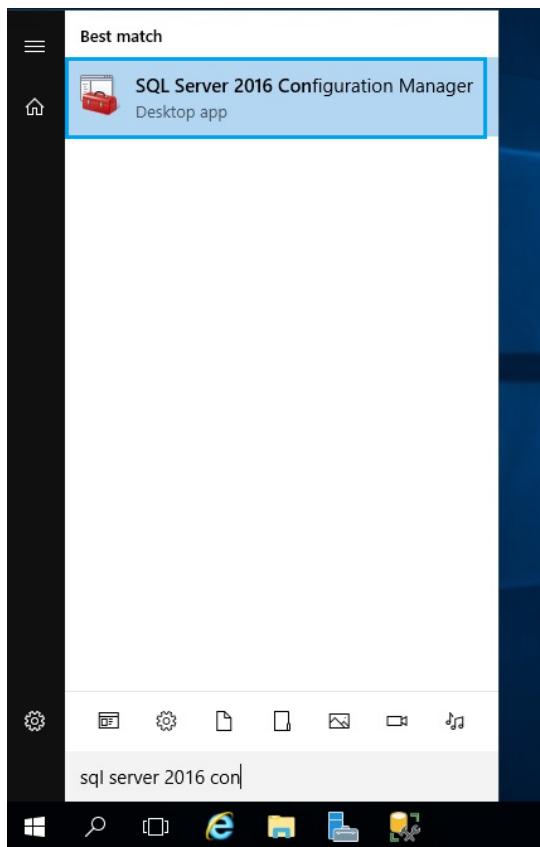


8. Right click on **User (created)** > Right click and select **properties** > click **Server Roles** > check the **sysadmin** box to give permission to the new user.

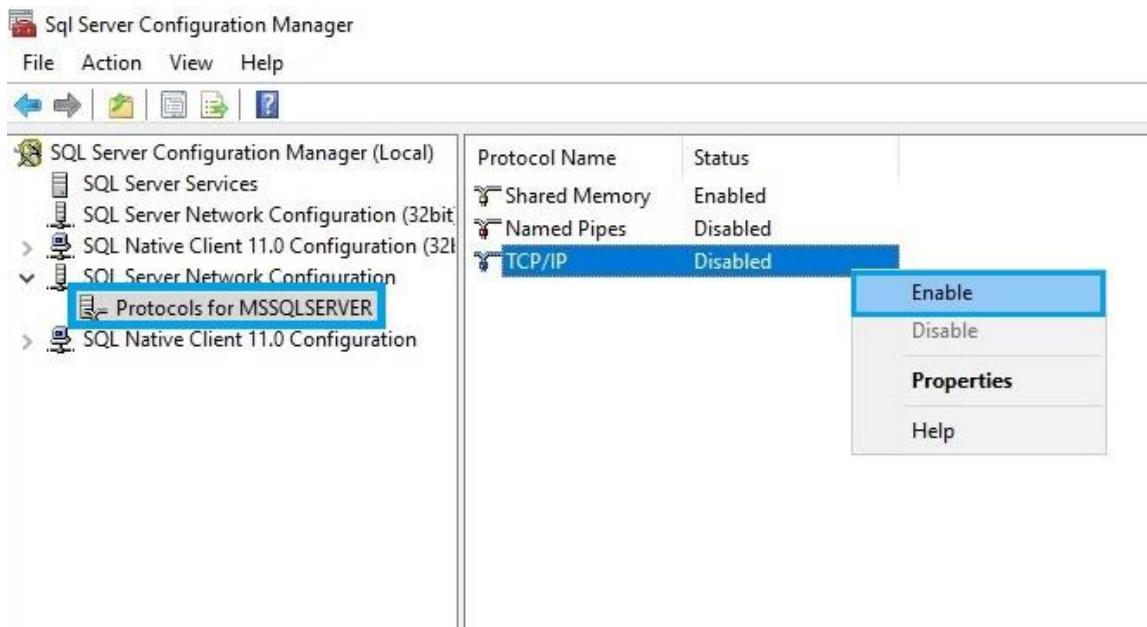


8.2. Enable TCP and Named Pipe in SQL Server Configuration Management

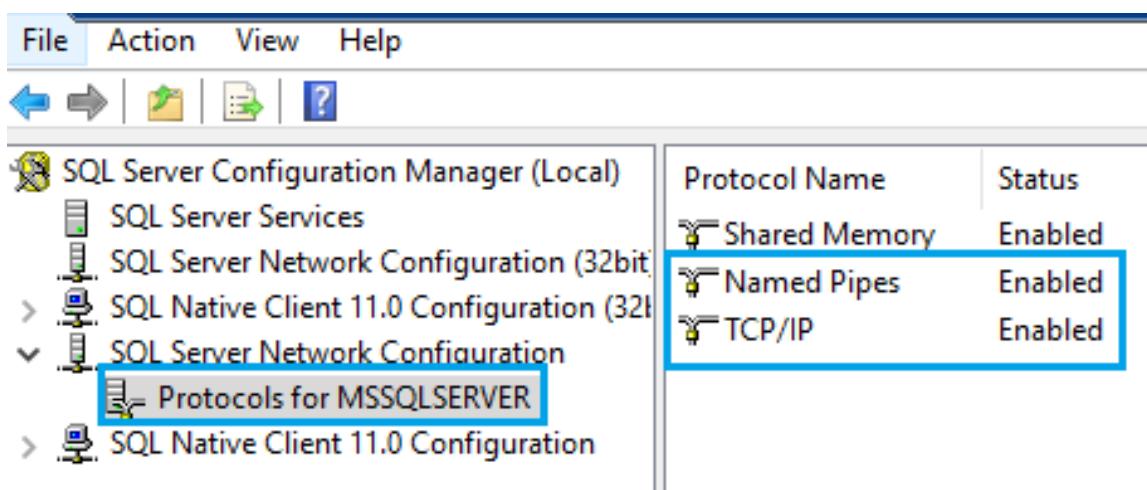
1. From the **Start** menu, navigate to **SQL Server 2016 Configuration Management**.



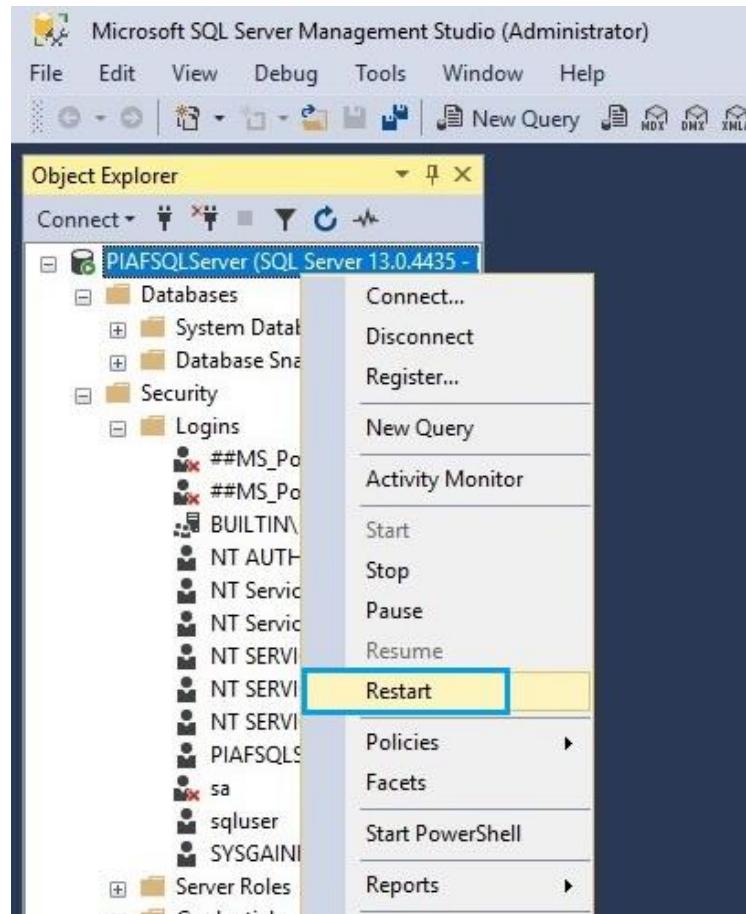
2. Click on **SQL Server Network Configuration > Protocols for MSSQLSERVER**.



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



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



9. Components of PI Server

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

PI Server is comprised of 3 Components:

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

9.1. PI Asset FrameWork (AF)

PI Asset Framework (AF) is a meta-data structure of data and an integral part of the PI Server. It allows you to build an asset model of the physical objects in your process and associate asset properties to your data. It is a single repository for asset-centric models, hierarchies, objects, and equipment.

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

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

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

9.1.1. Installation of PIAF Server

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

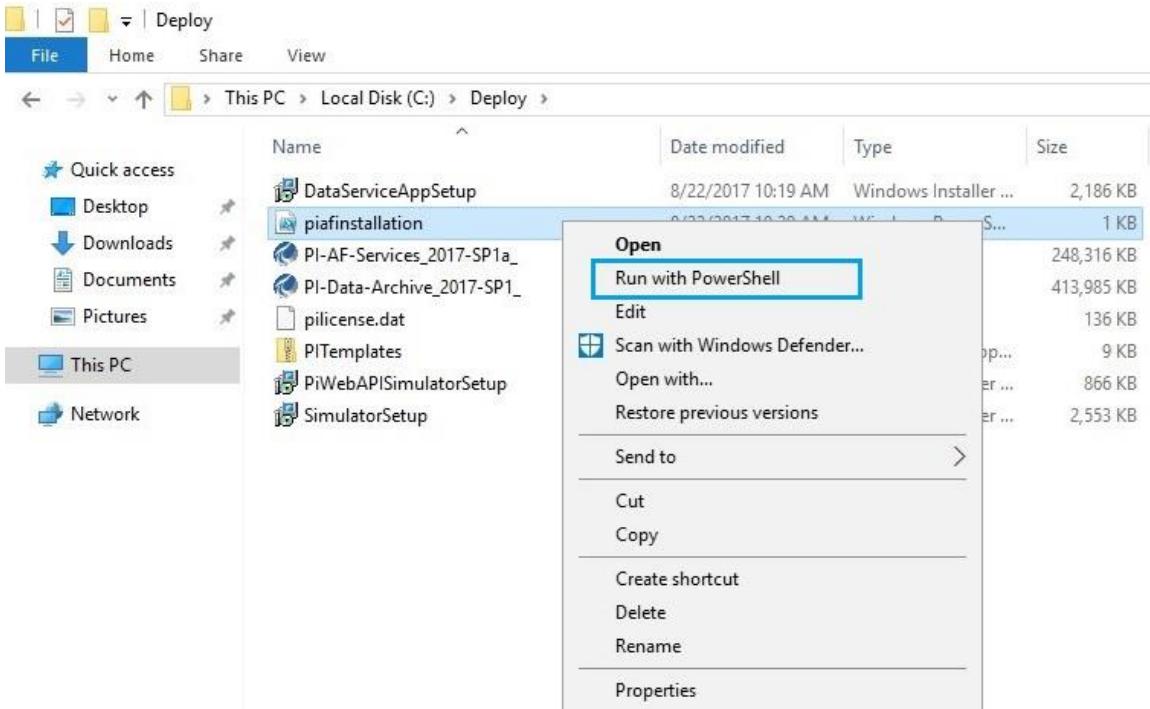
Outputs

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

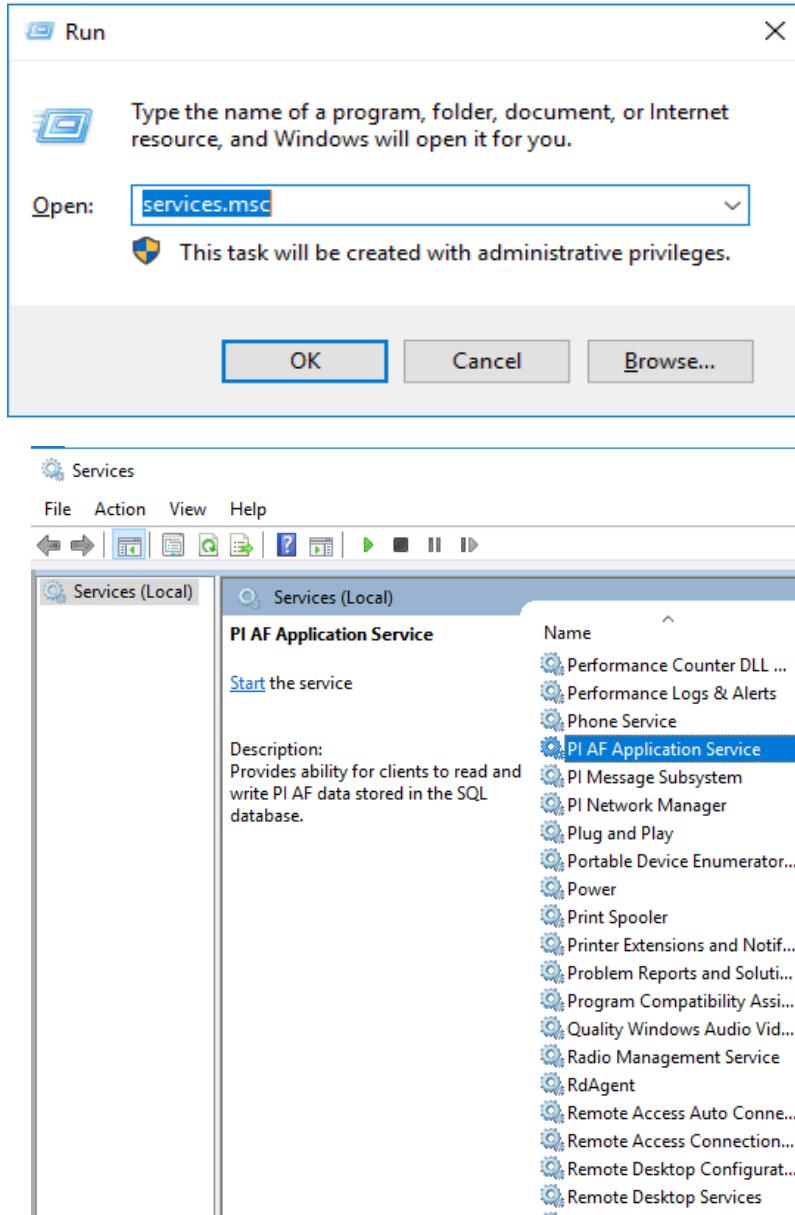


2. Navigate to **Local disk (C:) > Deploy** > Right click on **piafinstallation** > Open with Notepad. In the PowerShell script, edit the **adminuser** and **Password@1234** values to update them with your username and password from the PIAFSQLServer and then **save**. After that, right click on the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

```
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").



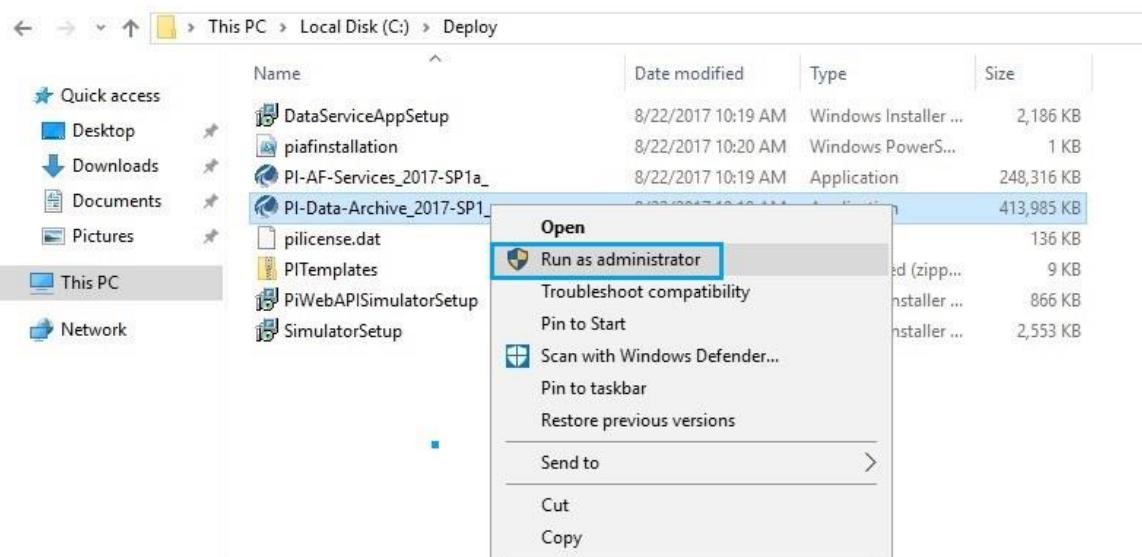
9.2. PI Data Archive (PIDA)

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.

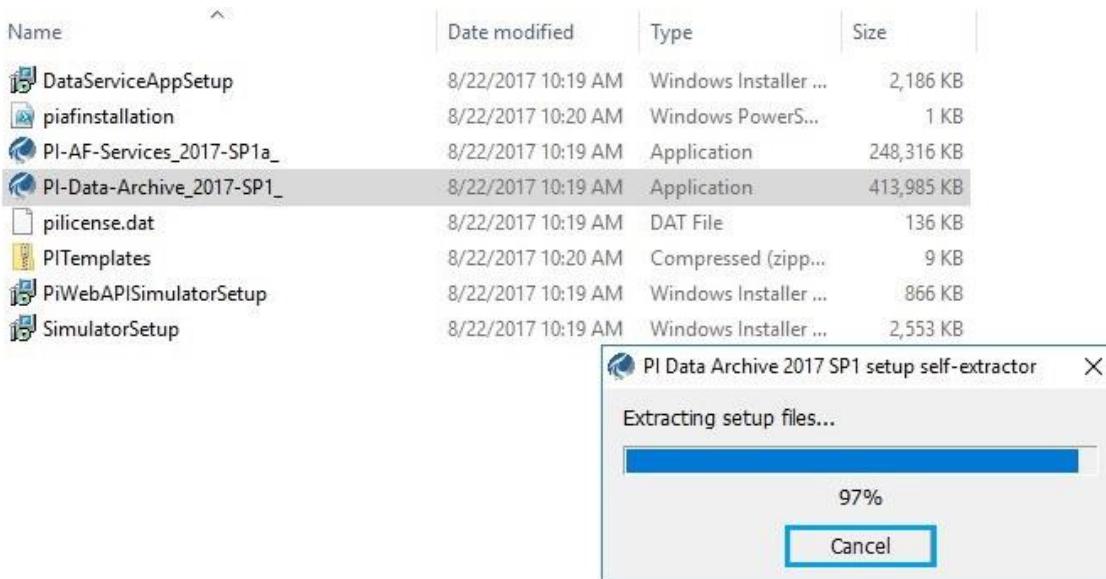
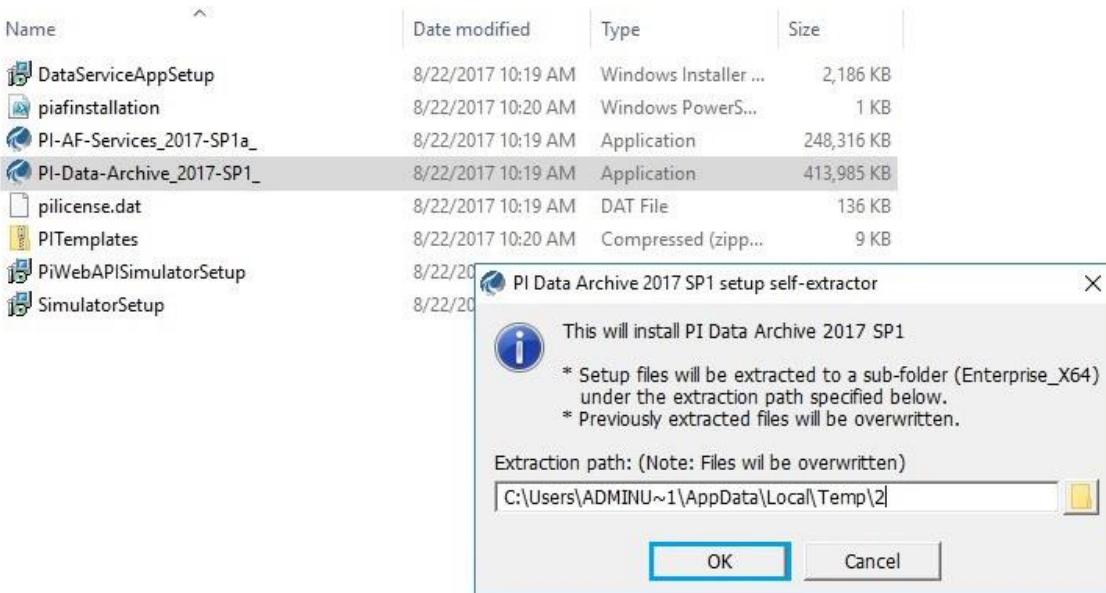
The PI Data Archive collects, stores, and organizes data from data sources, providing an information infrastructure. The PI Server also includes tools for analytics, alerts, and auditing. The PI Server may be connected to almost any existing automation, lab, or information system. Operators, engineers,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

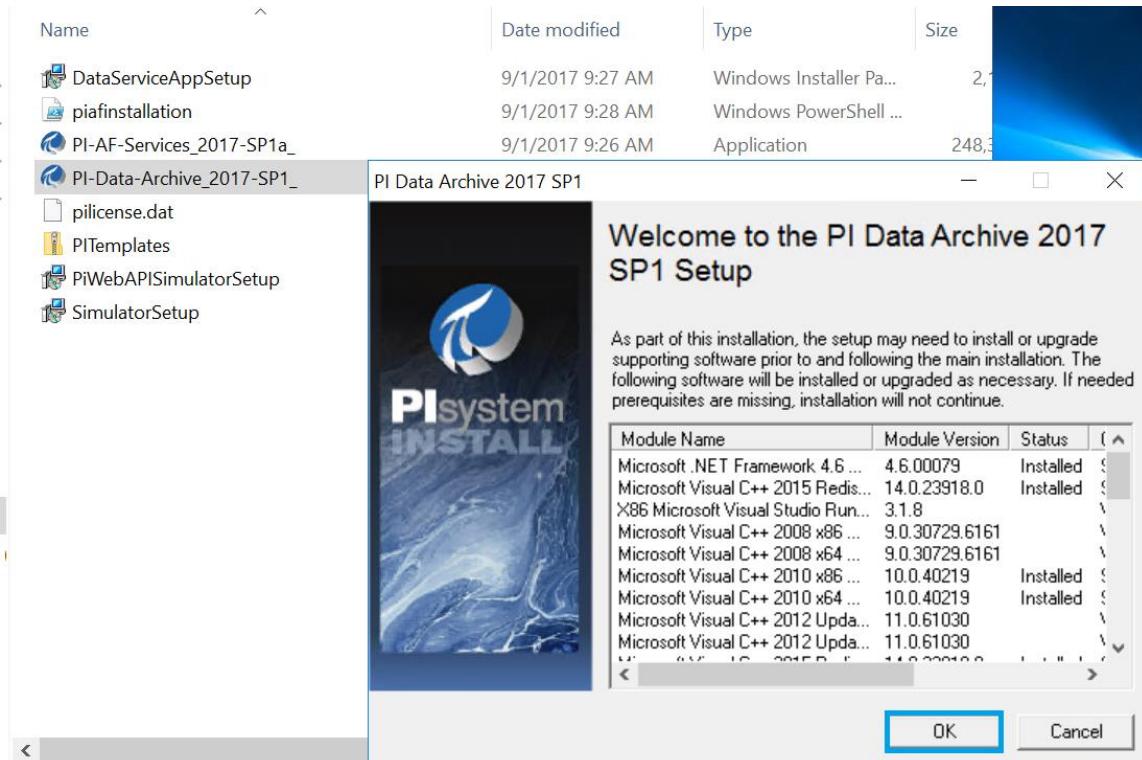
1. Navigate to **Local disk (C:)** > **Deploy** > select **PI-Data-archive_2017-SP1** > right click and **Run as administrator**.



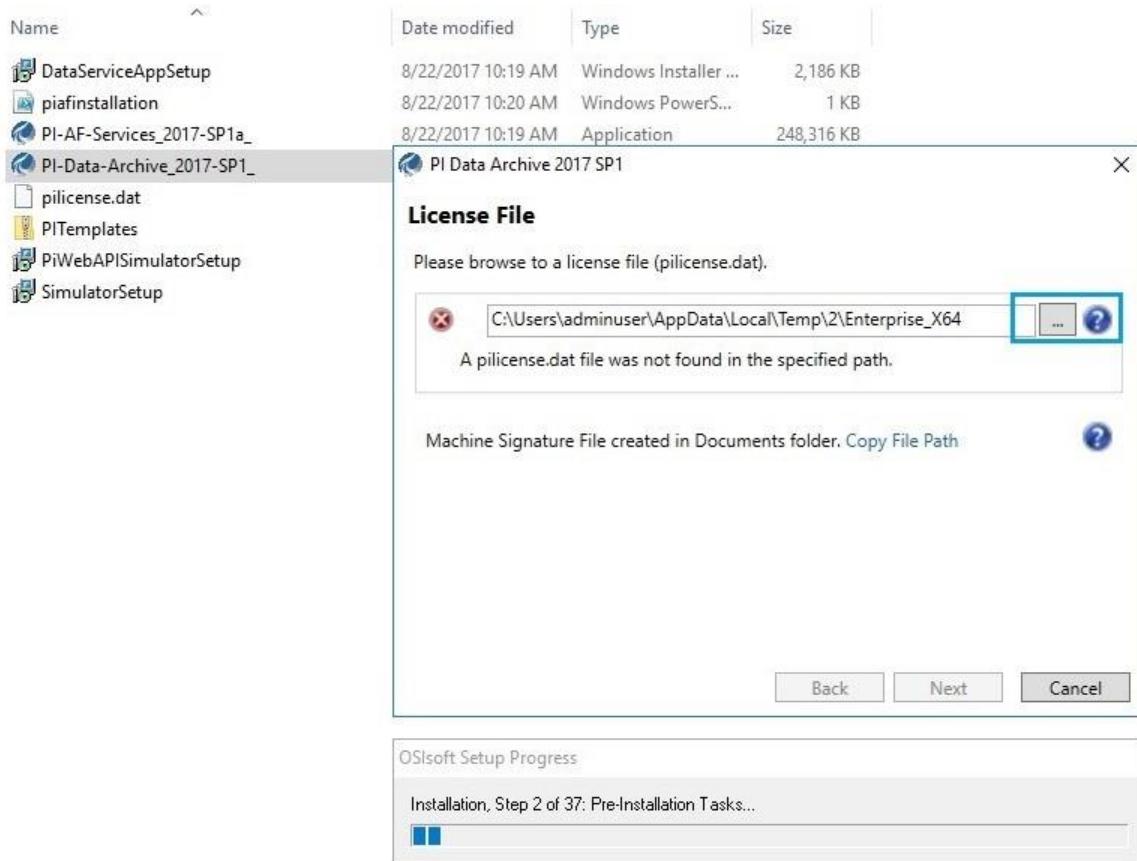
2. Click on **OK**.



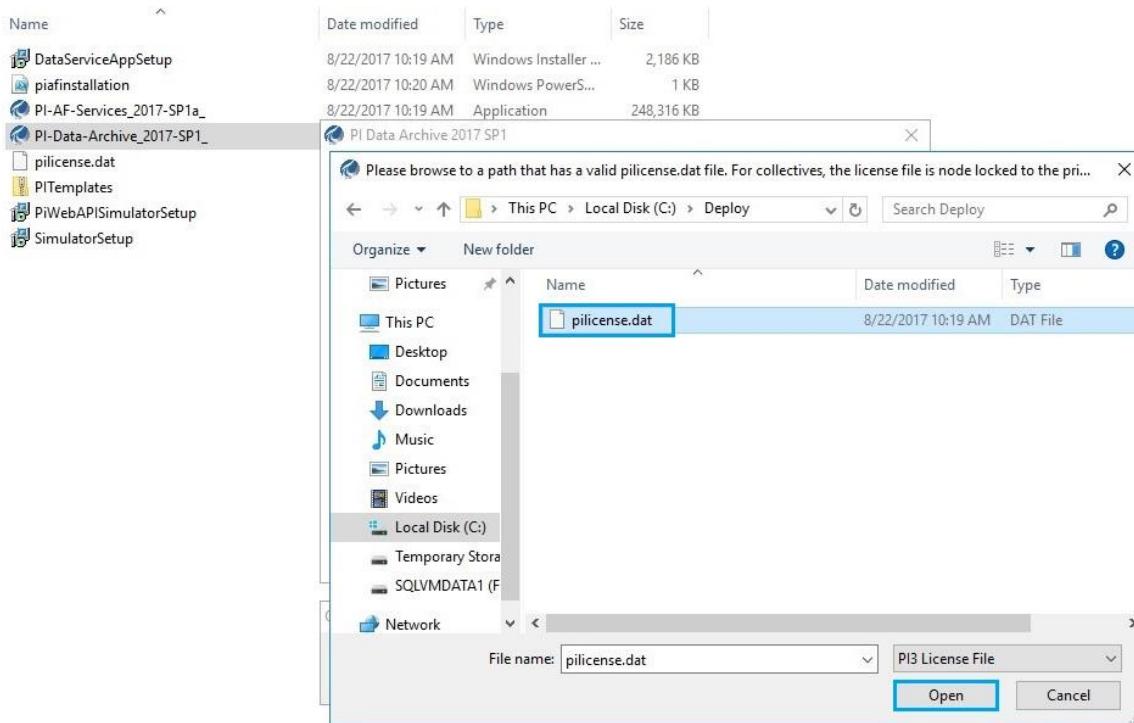
3. Click on **OK**.



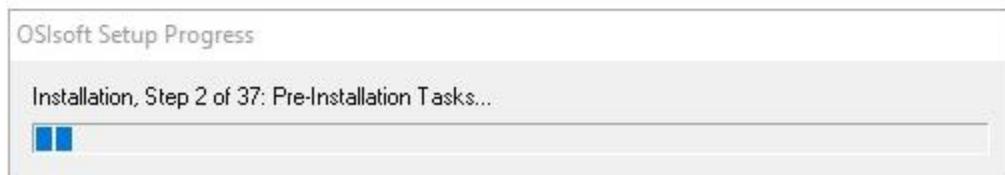
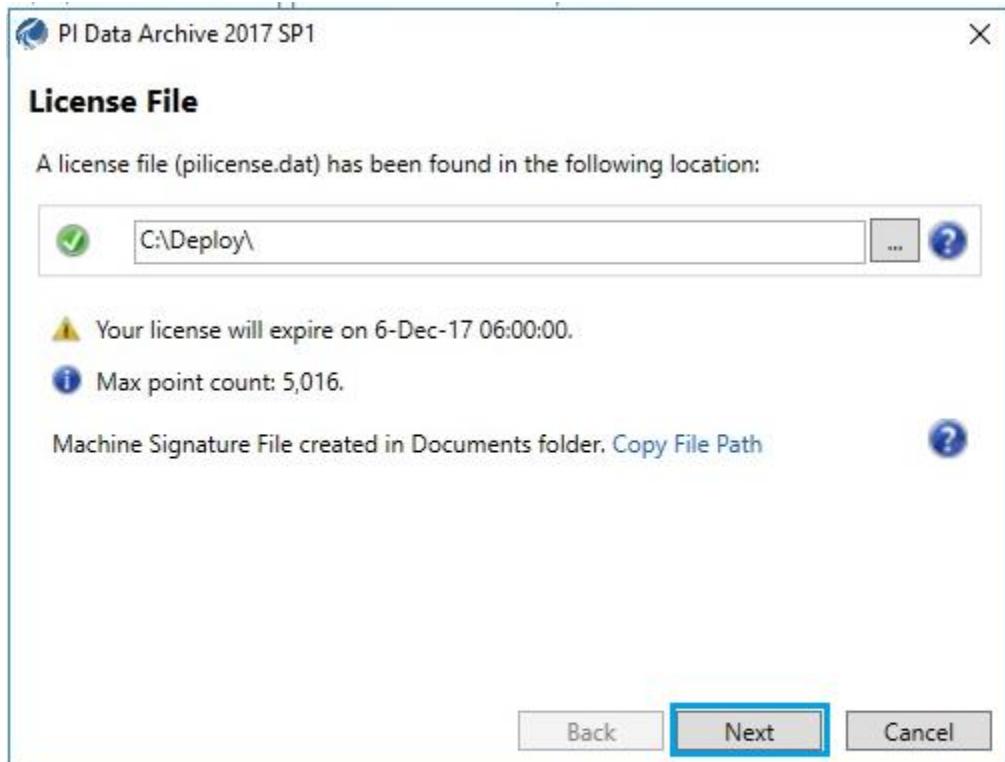
4. After completion of extracting setup files, click on **OK**.



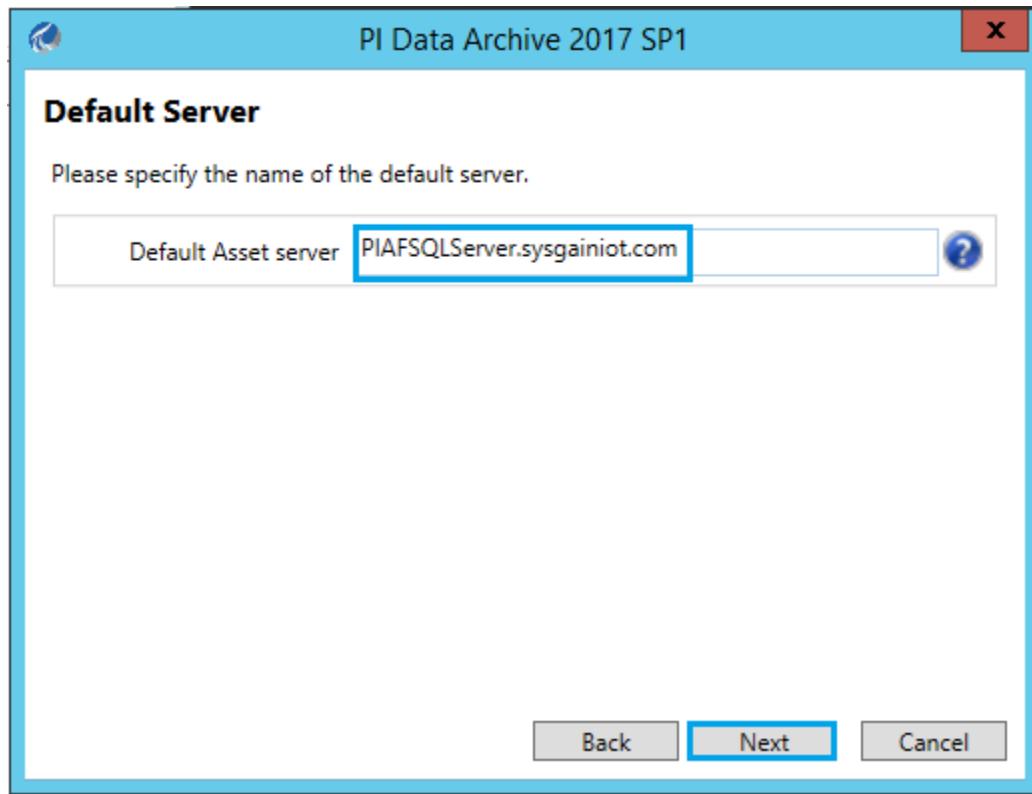
5. Click on the browse option, then navigate to the **Local disk (C:) > Deploy** > select **pilicense.dat** and click on **Open**.



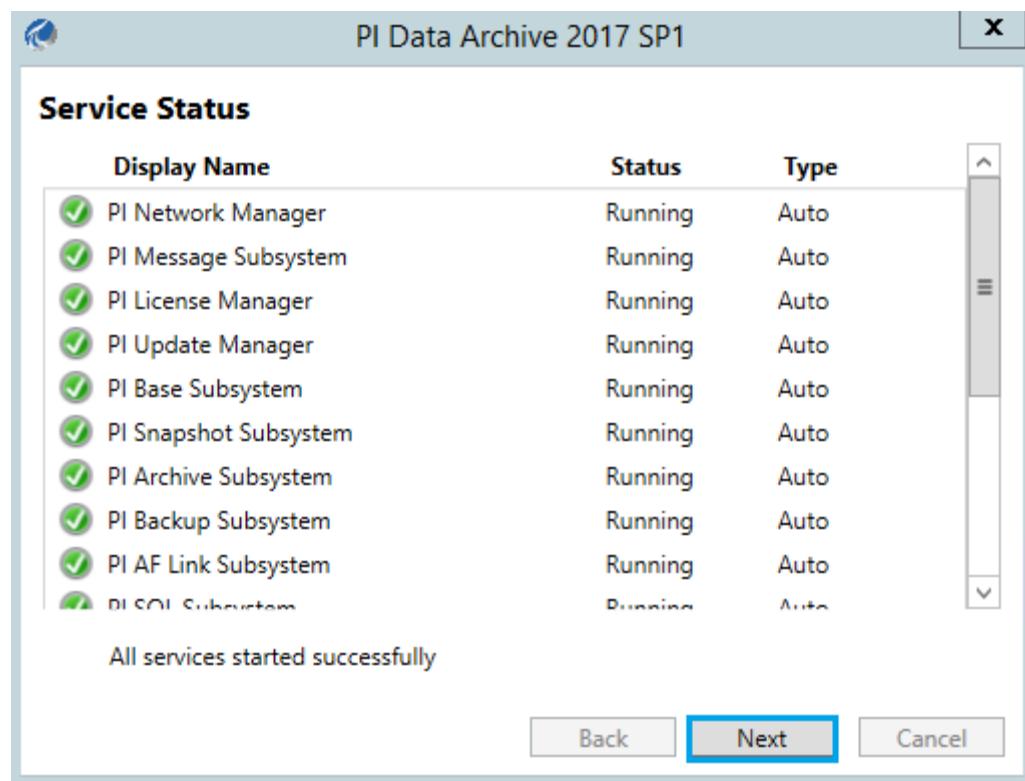
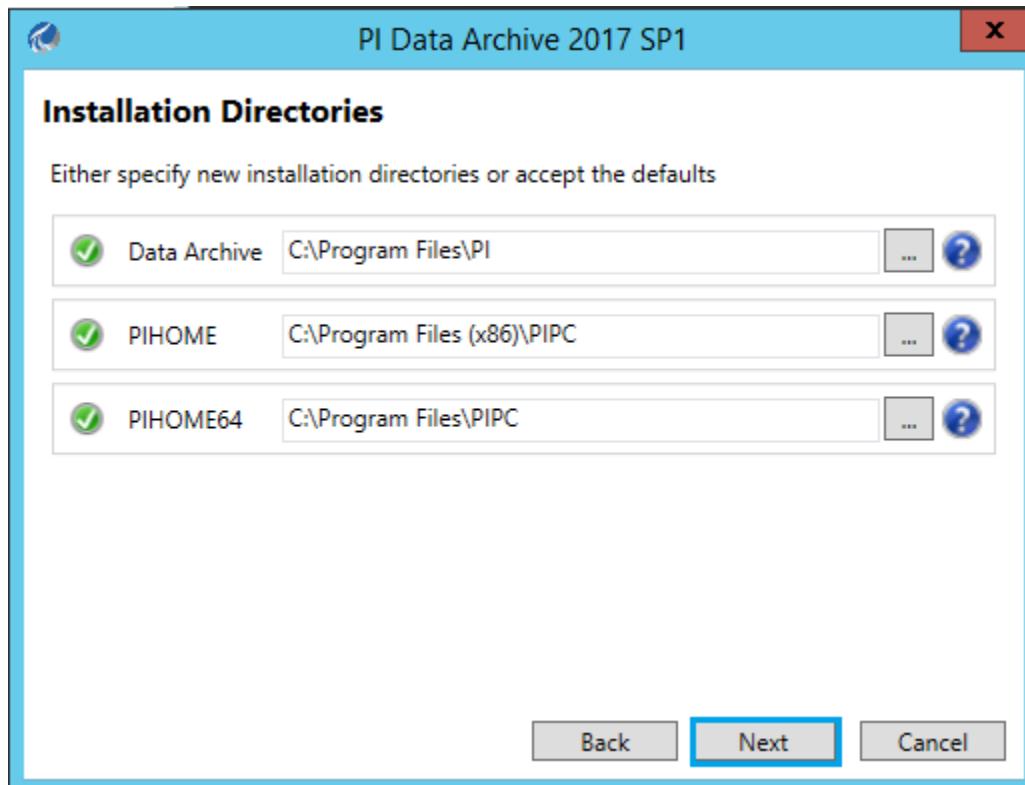
6. After that, click on **Next**.



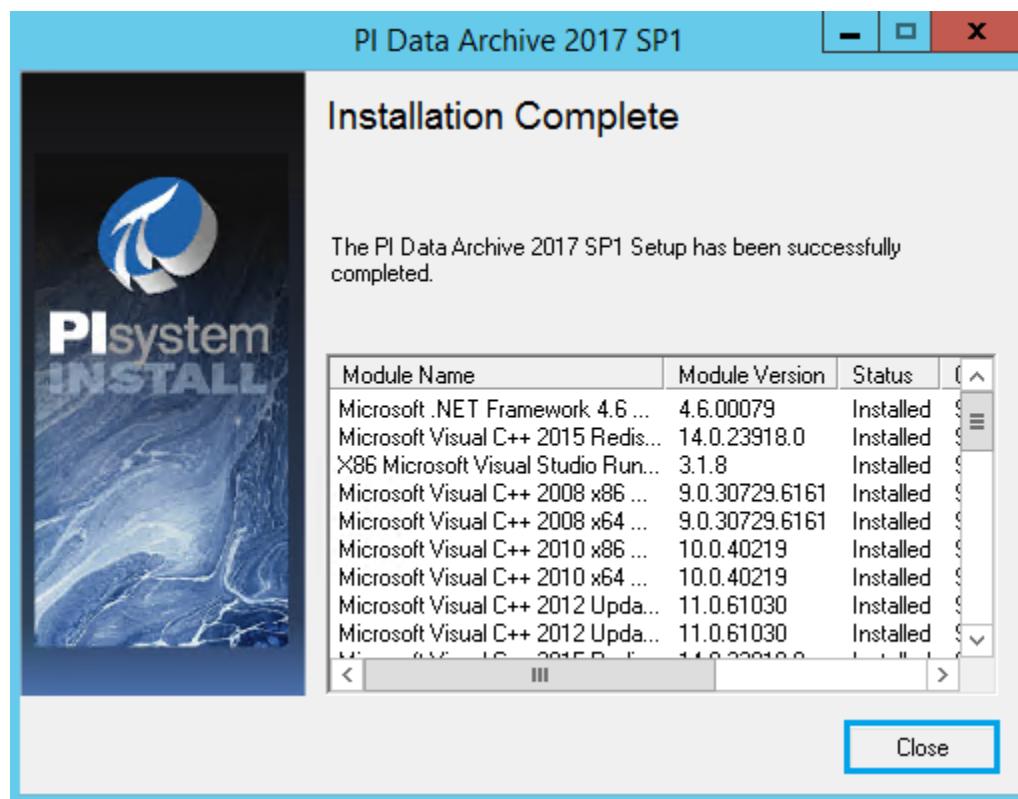
7. Add the domain name to the **Default Asset server** and click on **Next**.



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

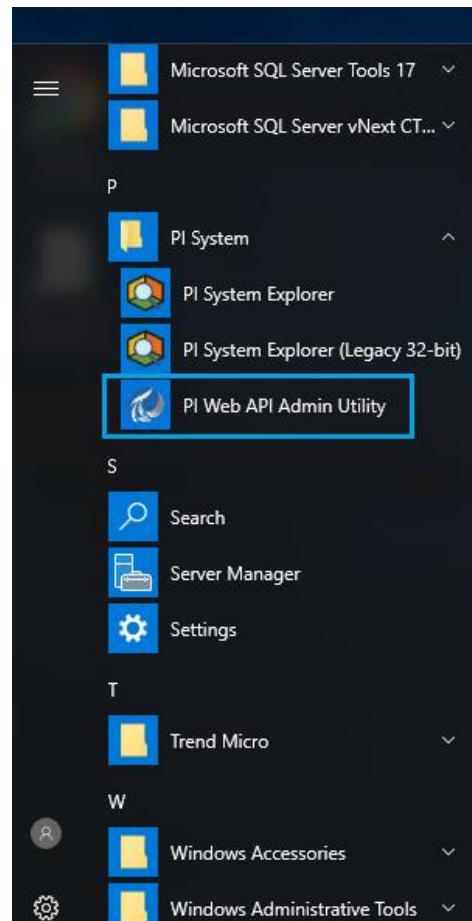


9. Click on **Close** once the installation is completed.

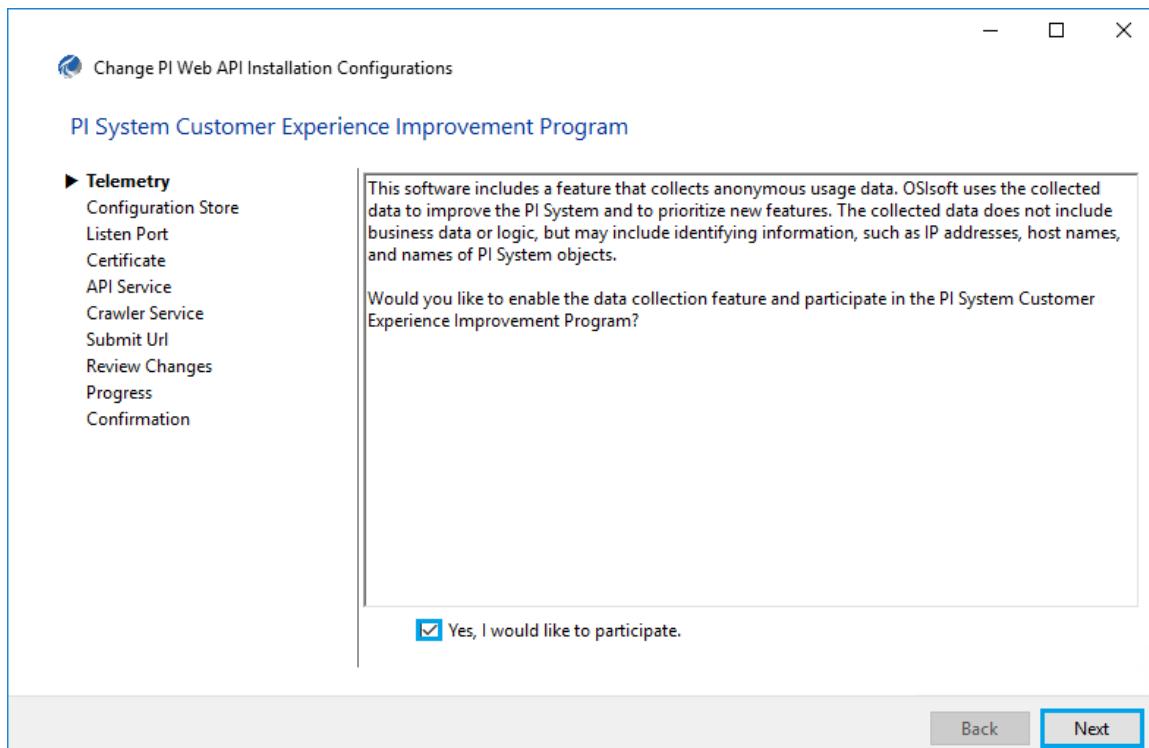


9.3. PI Web API Utility

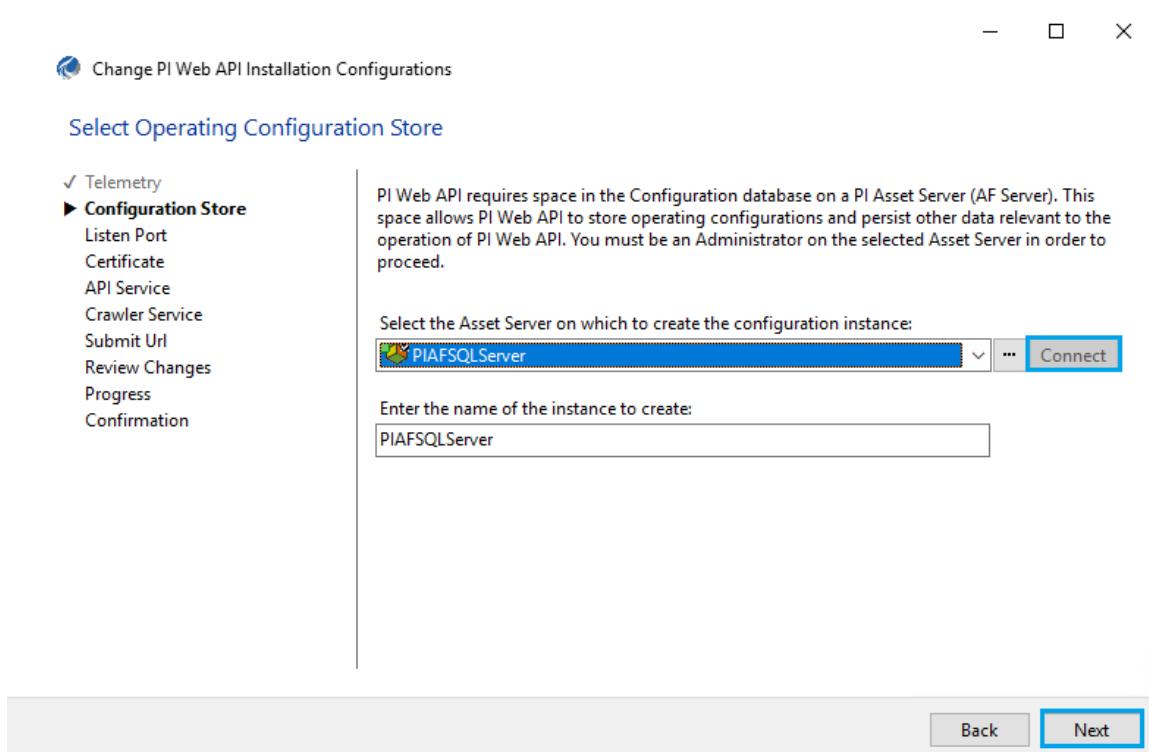
1. Navigate to **PI System > PI Web API Admin Utility** from the Start menu.



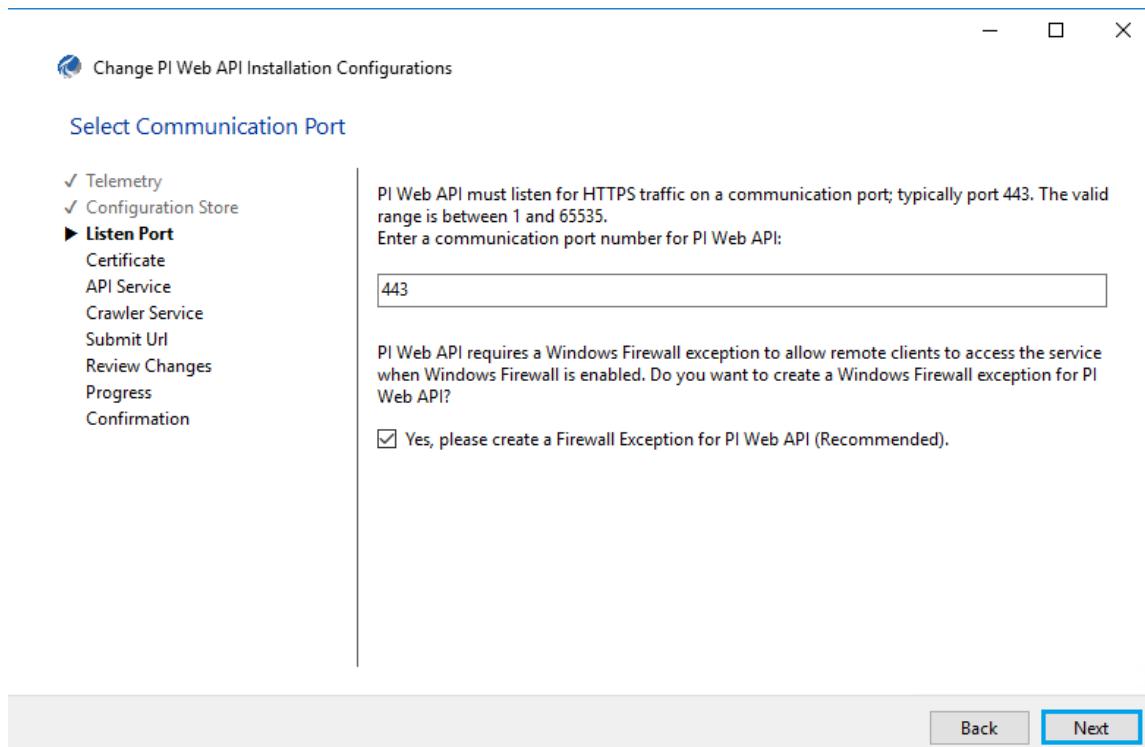
2. Check the **Yes, I would like to participate** dialog box and click on **Next**.



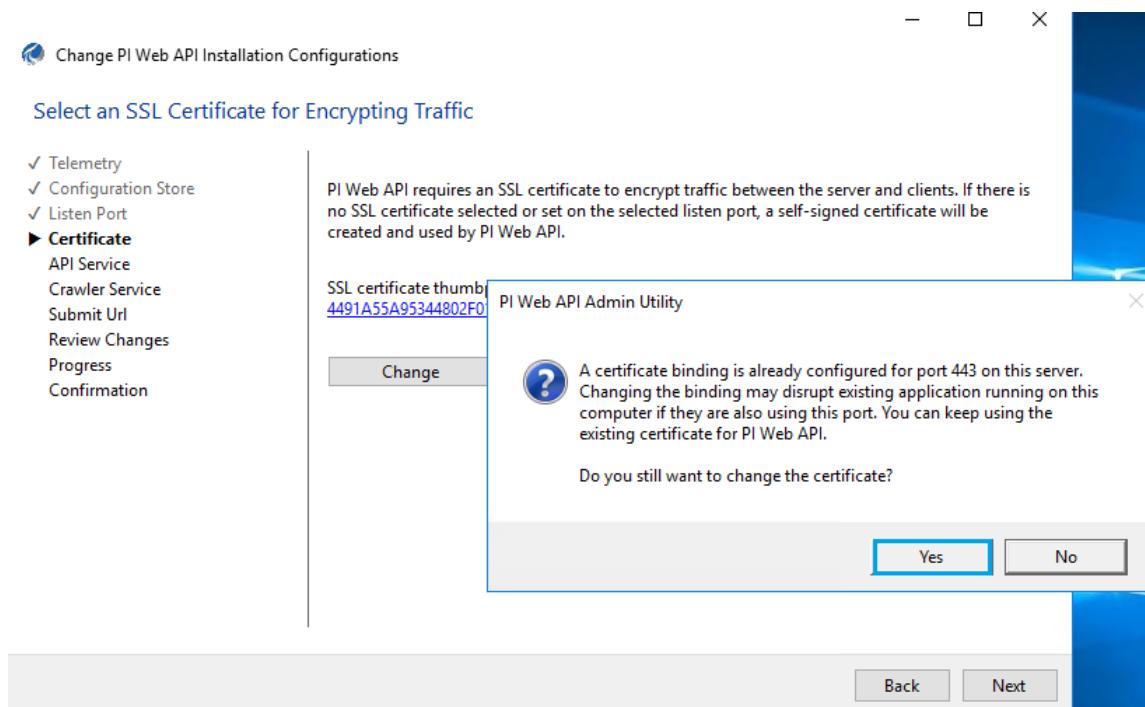
3. Select **Connect** and click on **Next**.



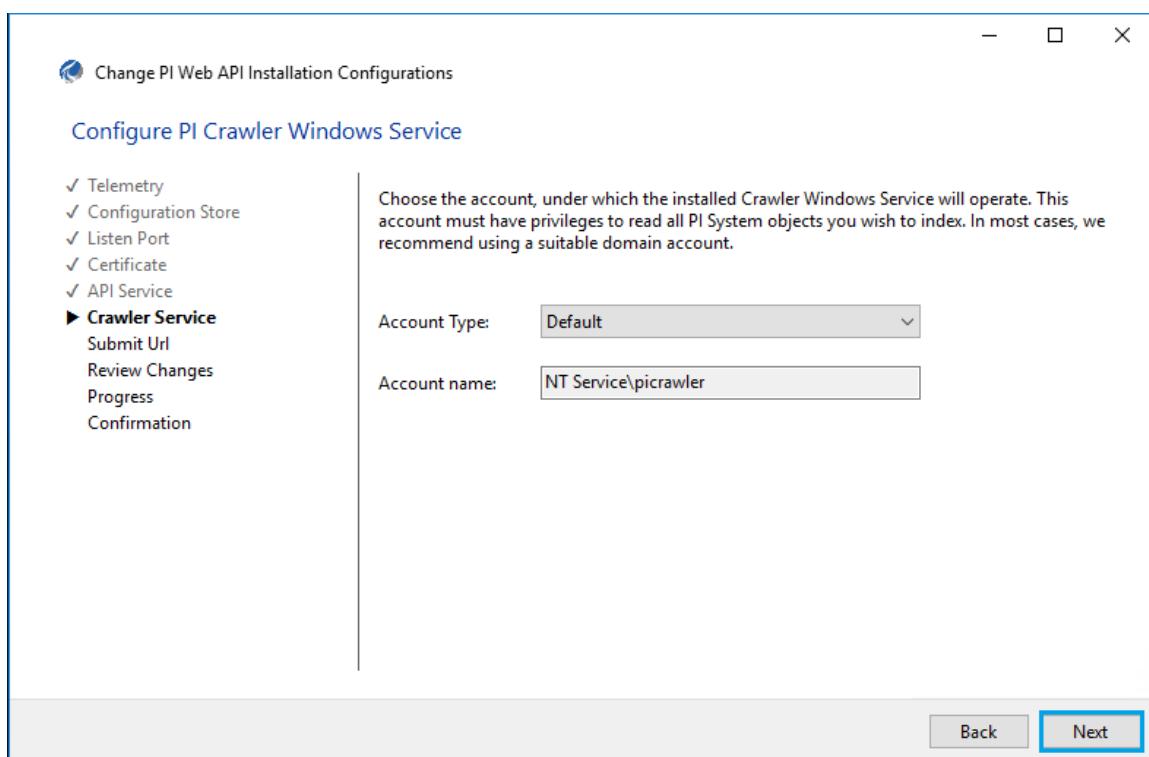
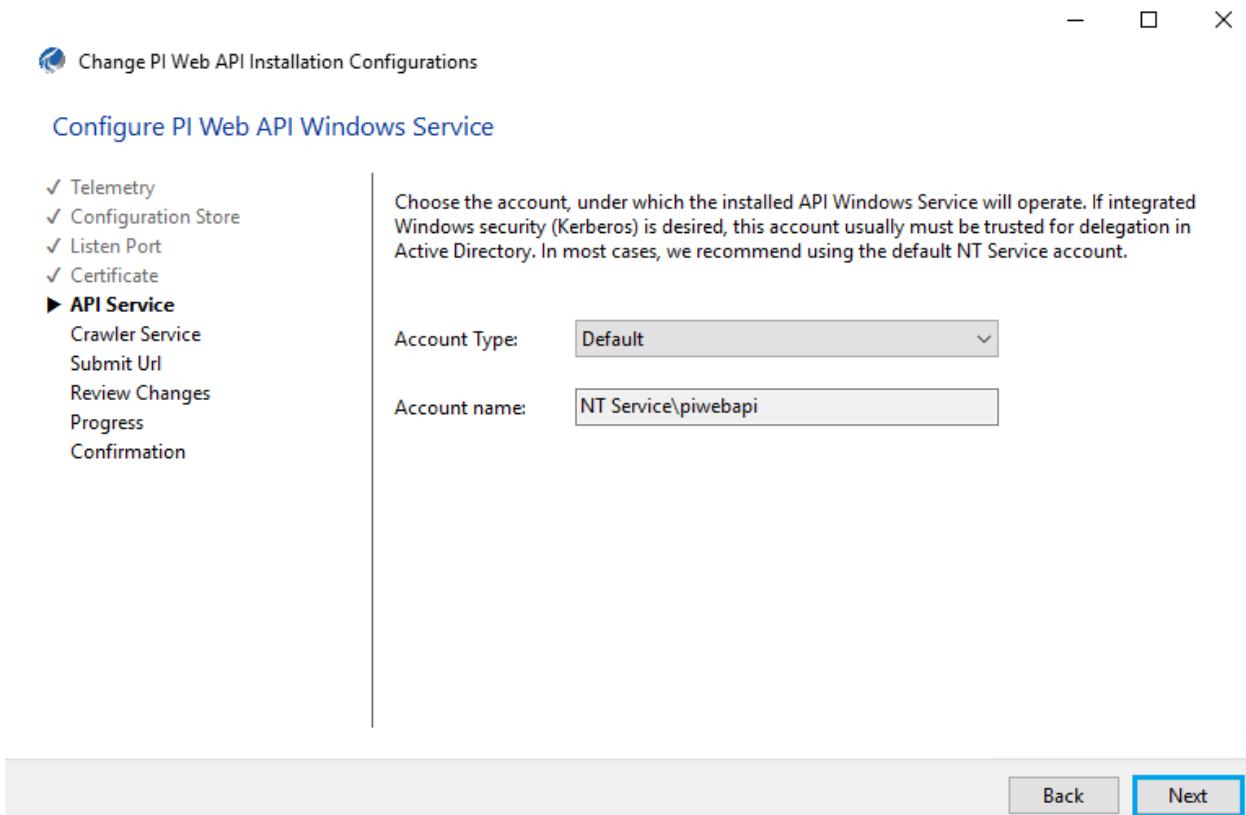
4. Click on **Next**.



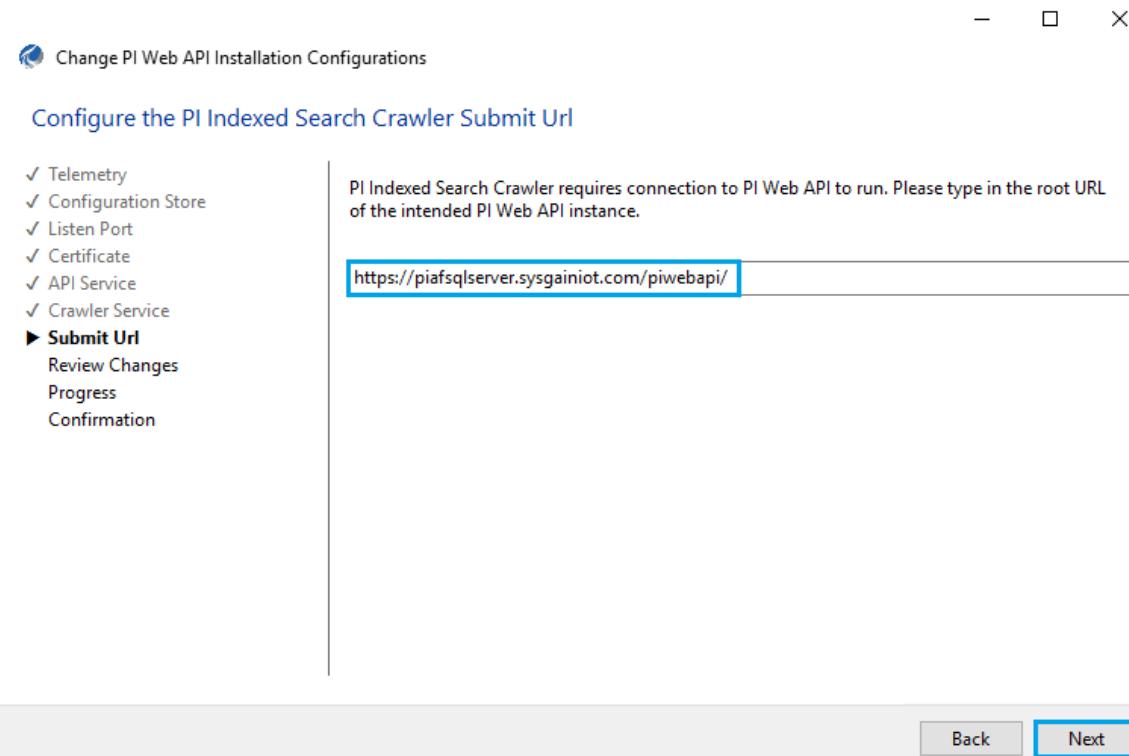
5. Click on **Remove** to remove the certificate and then click on **Yes**.



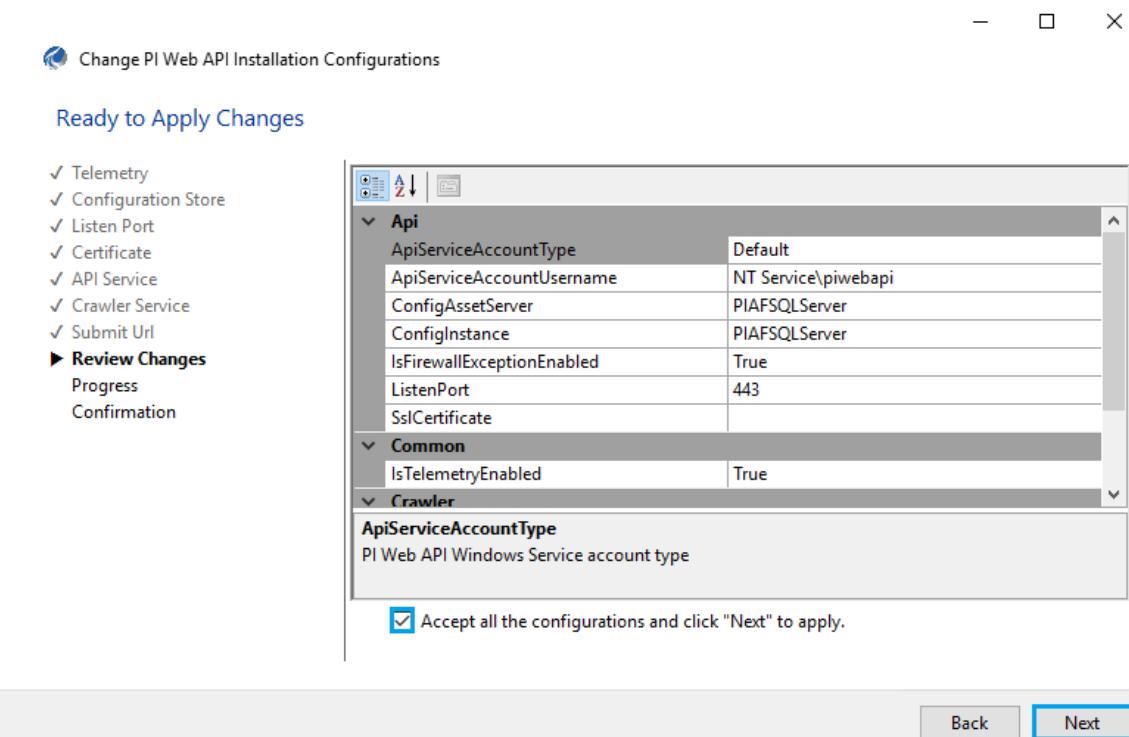
6. Configure **API Service** and **Crawler service** and click **Next**.

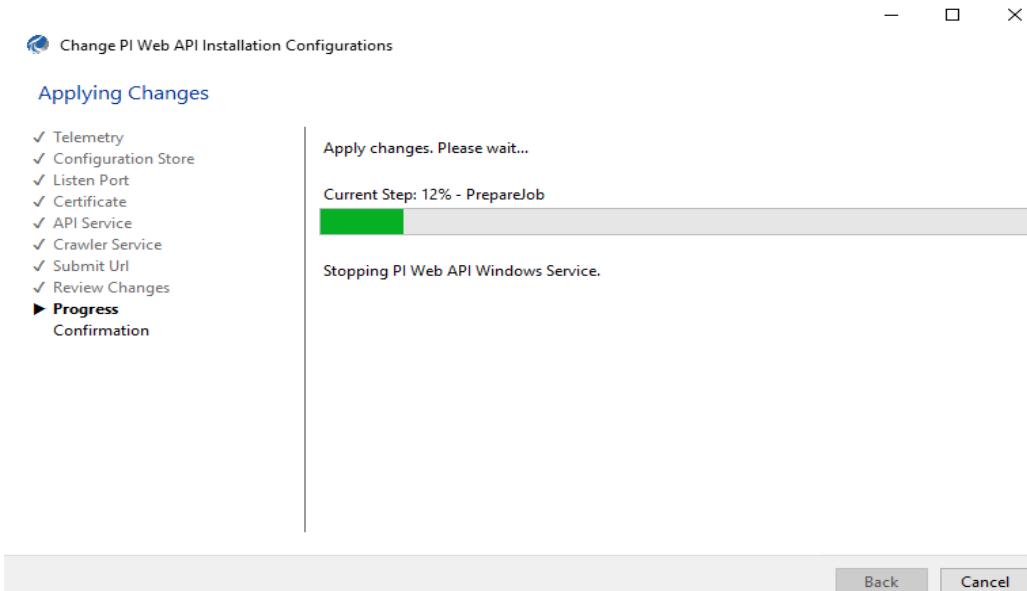


7. Note down the **Submit URL**.

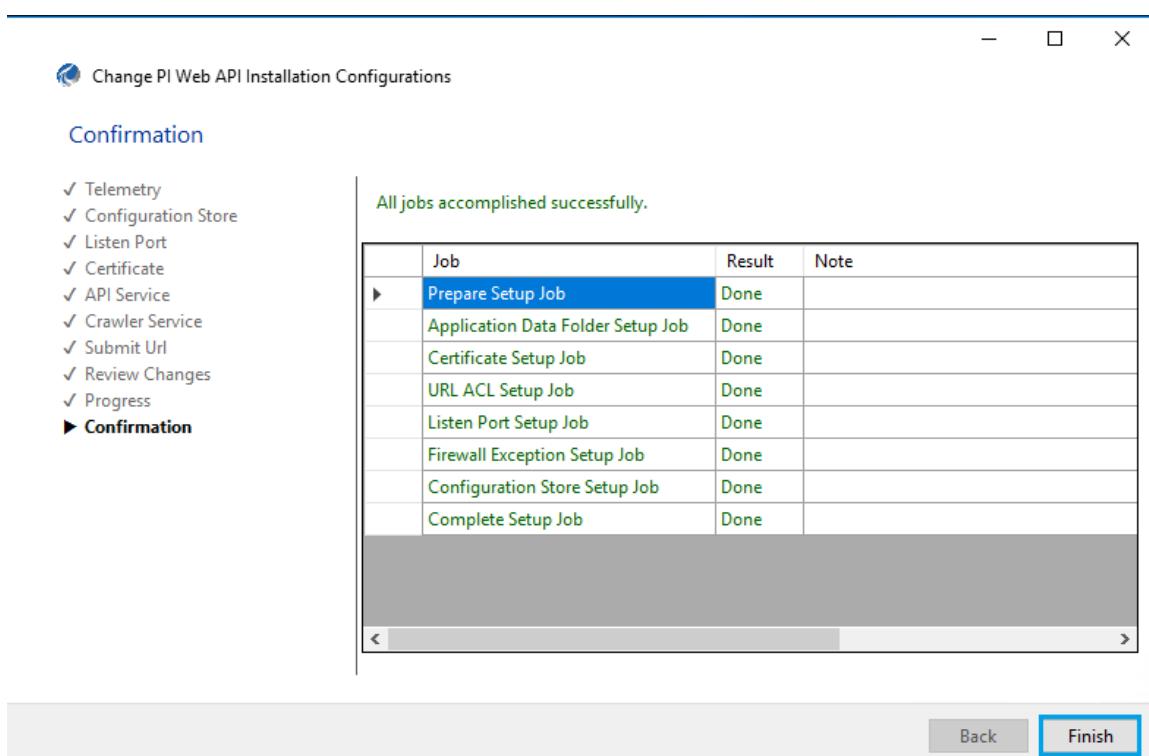


8. Check **Accept all the configurations** and click on **Next**.



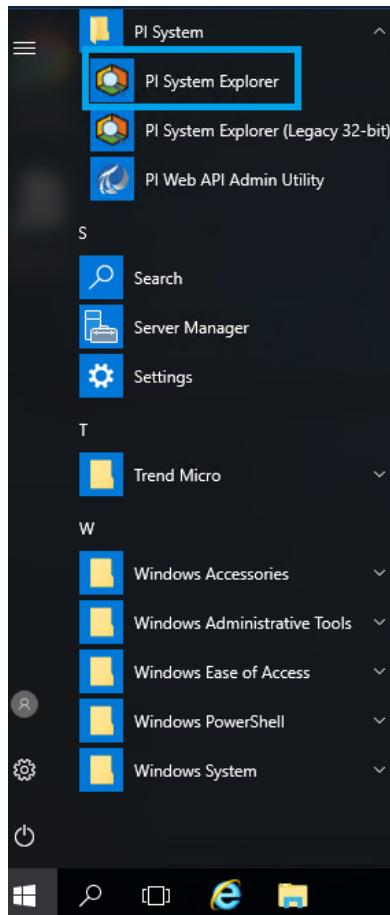


9. Click on **Finish**.

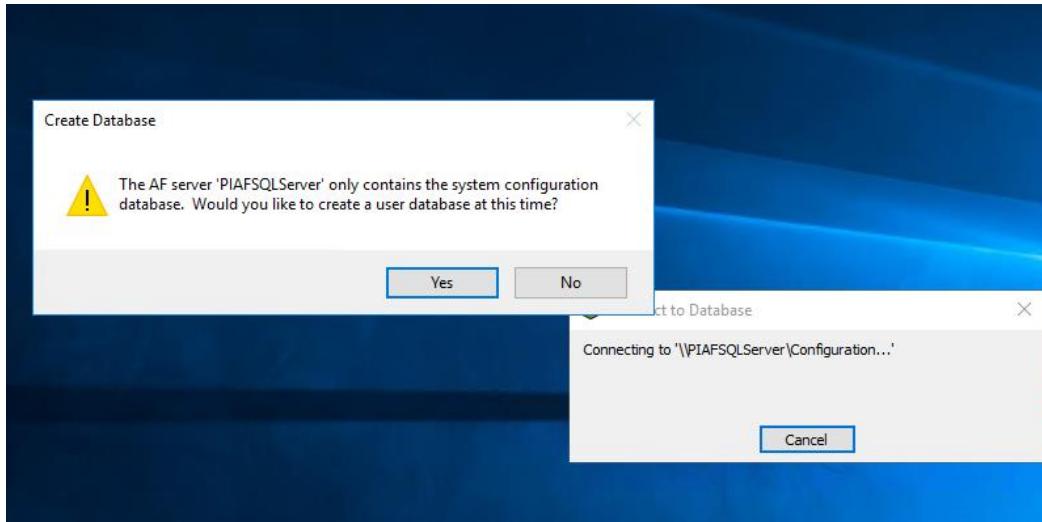


9.4. Creation of Database in PI System Explorer

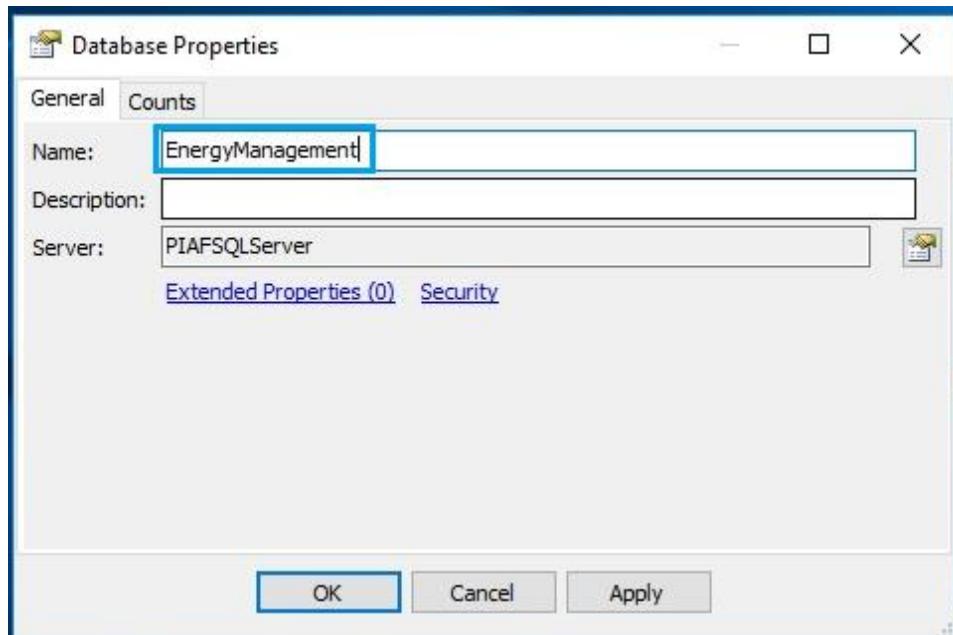
18. On the PIAFSQL machine, Navigate to **PI System Explorer** in PI System folder from the Start menu.



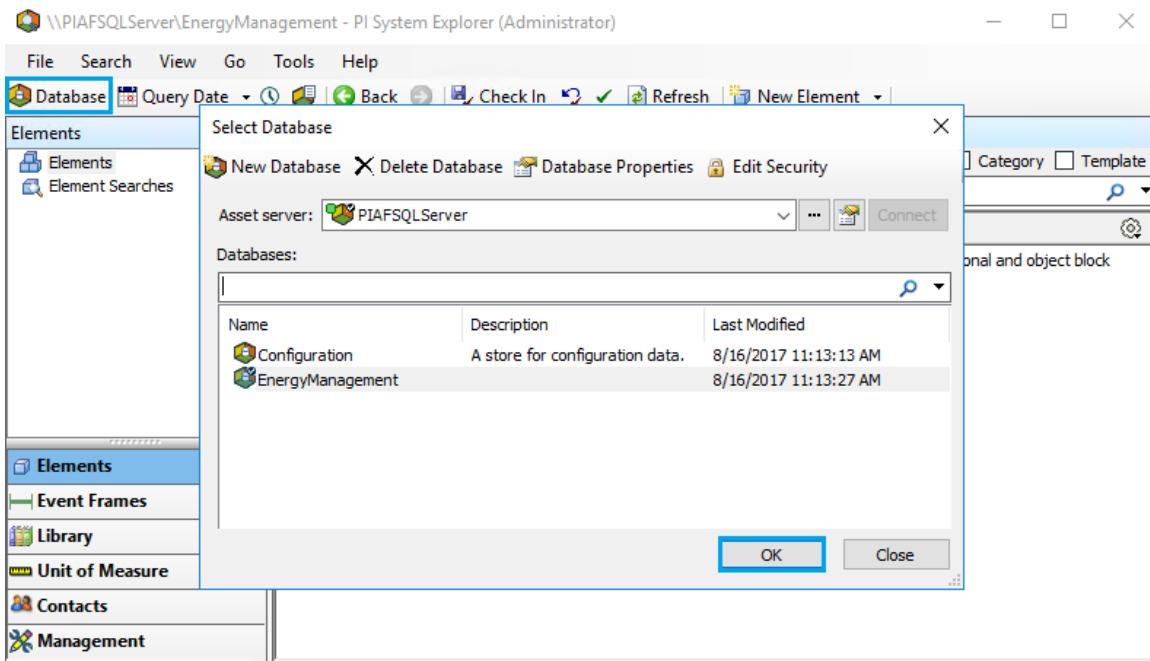
19. Two popups show up, **Connect to Database** and **Create Database**. Click **Yes** on the **Create Database** popup.



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

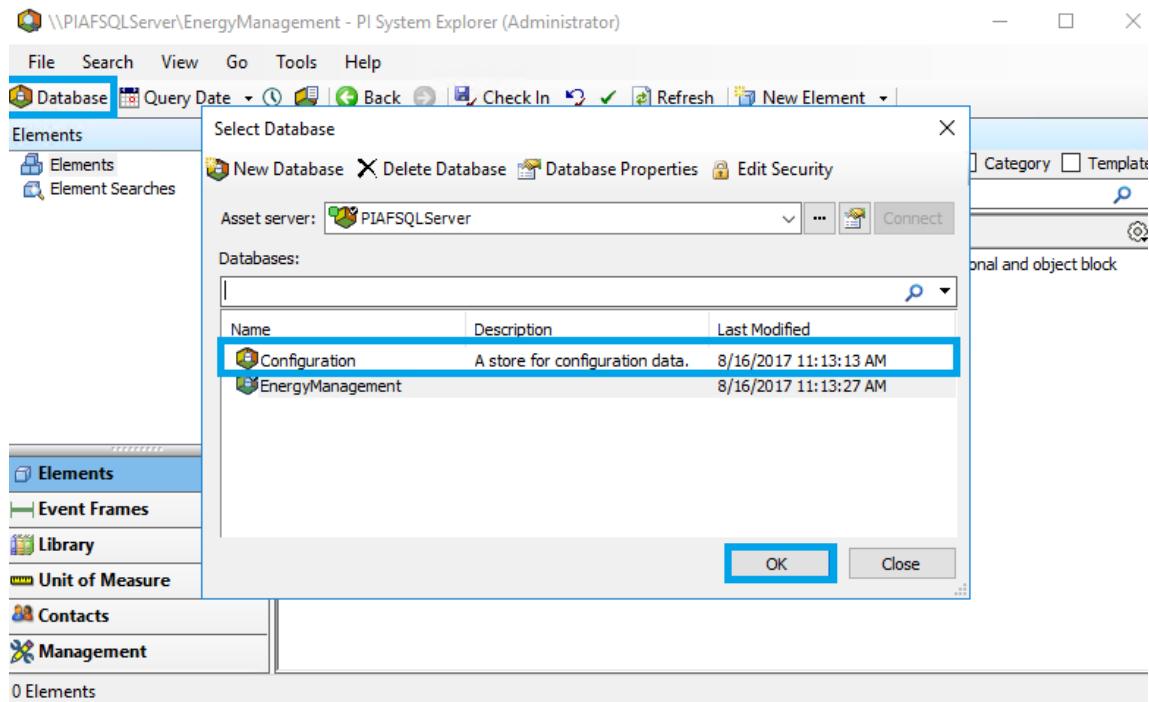


21. Navigate to **PI System Explorer**, click on **Database** to view the created database and click on **OK**.

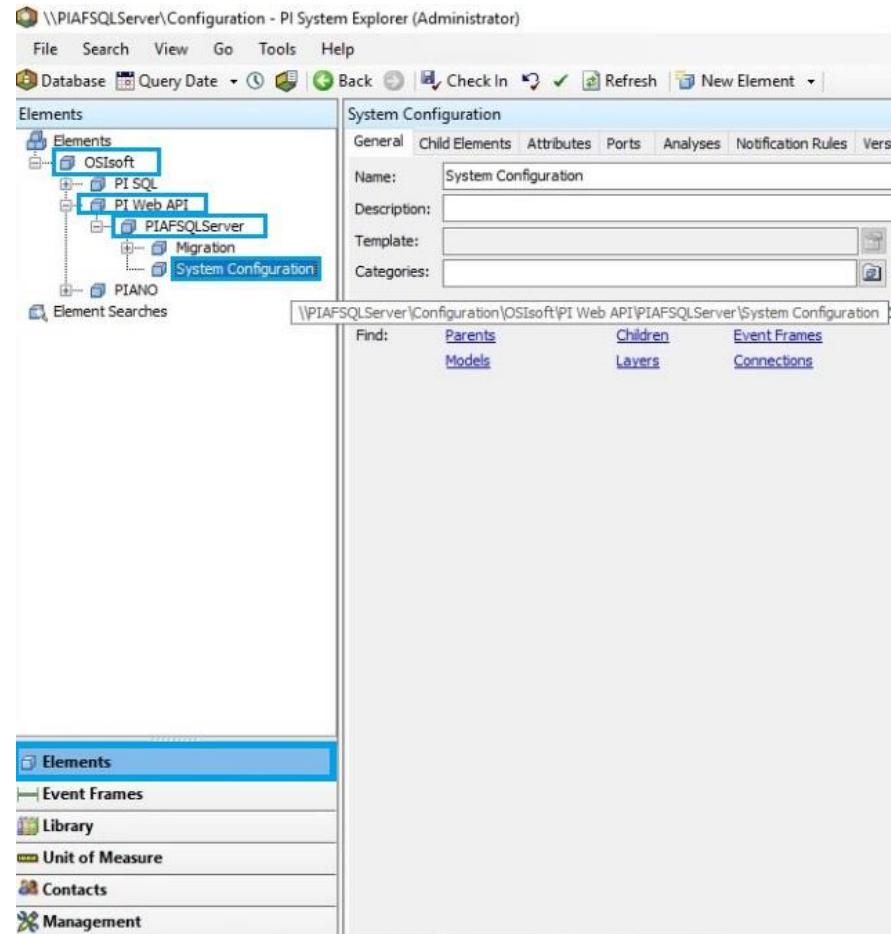


9.5. System Configuration in PI System Explorer

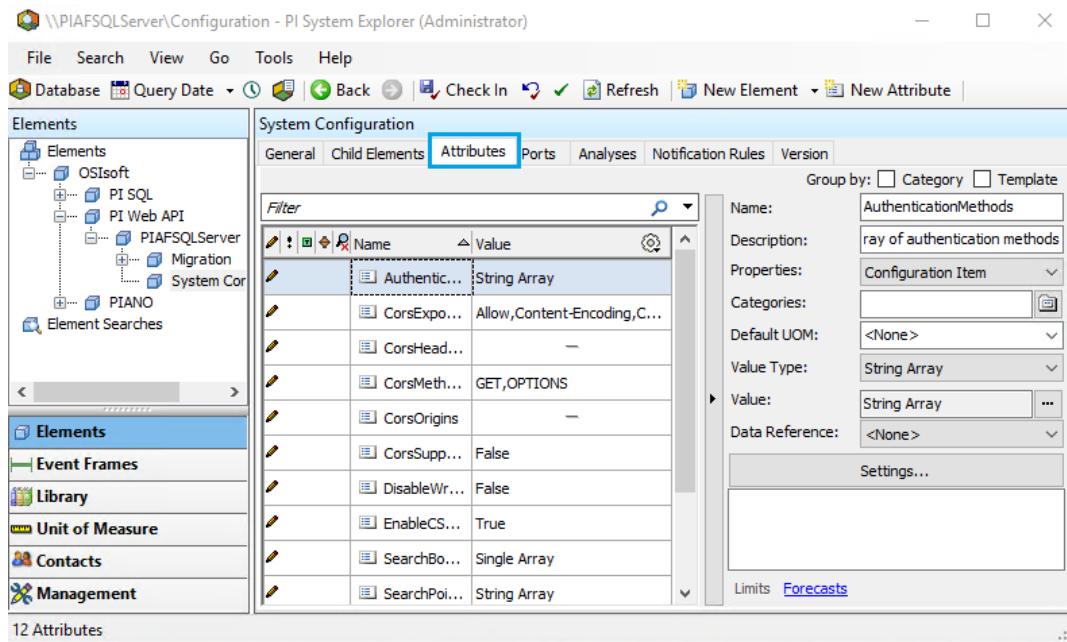
1. Navigate to **PI System Explorer** > Click on **Database** > click **Configuration** under Databases section. Click **OK**.



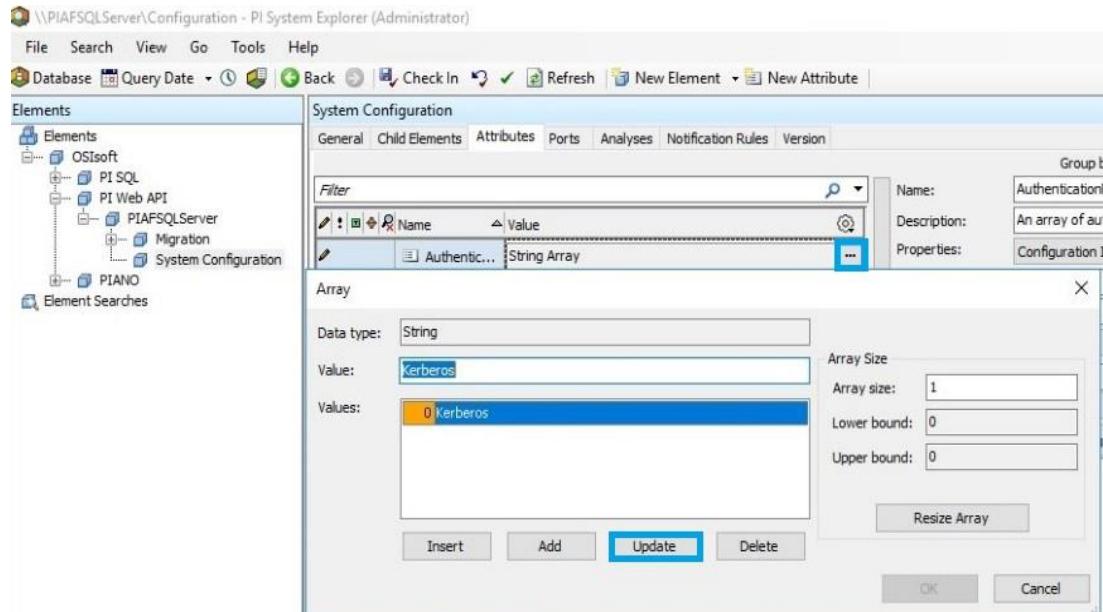
2. Click on **Elements** and navigate to **OSISoft > PI Web API > PIAFSQLServer > System Configuration.**



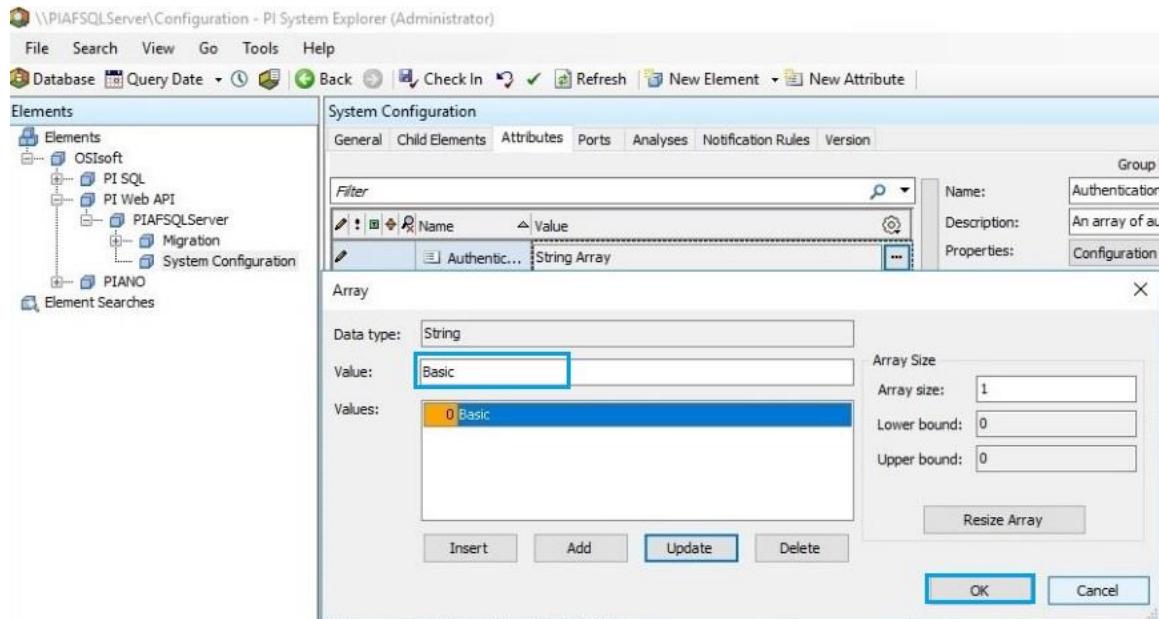
3. Click on **Attributes**.



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

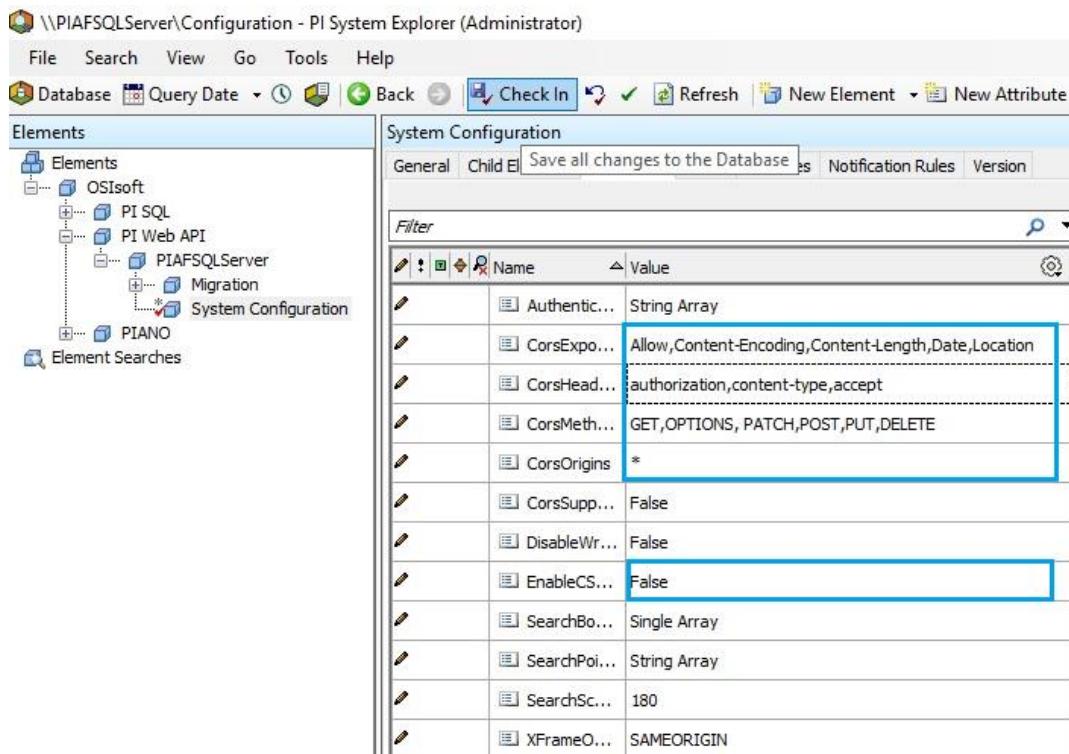


5. Click on **Update**, then **OK**.

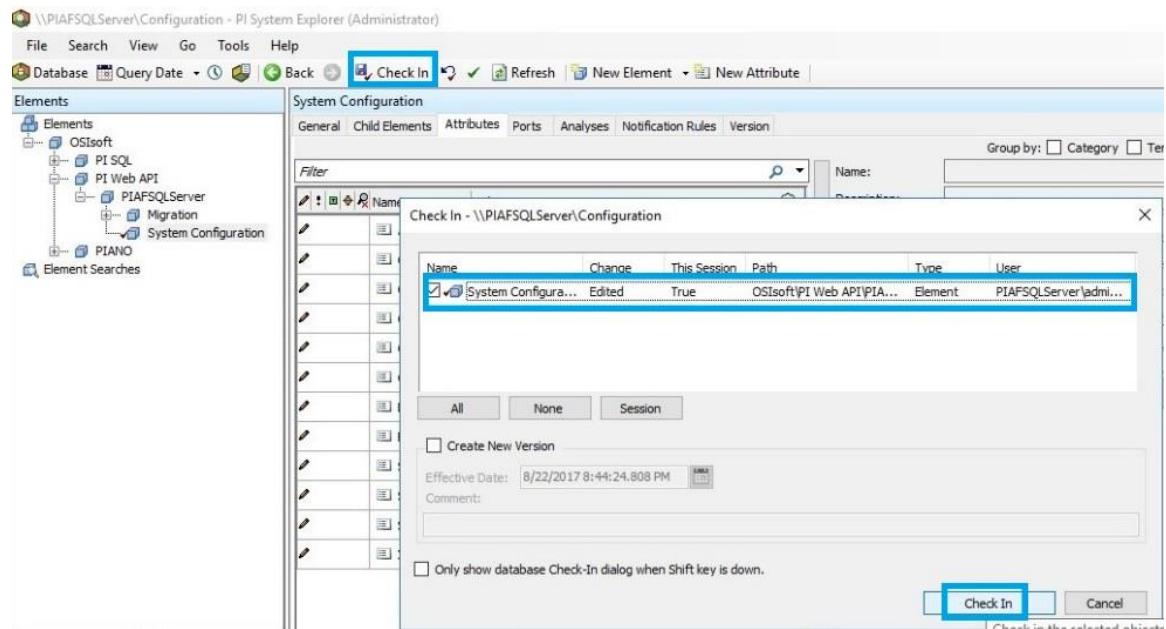


6. Similarly, change the following values:

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

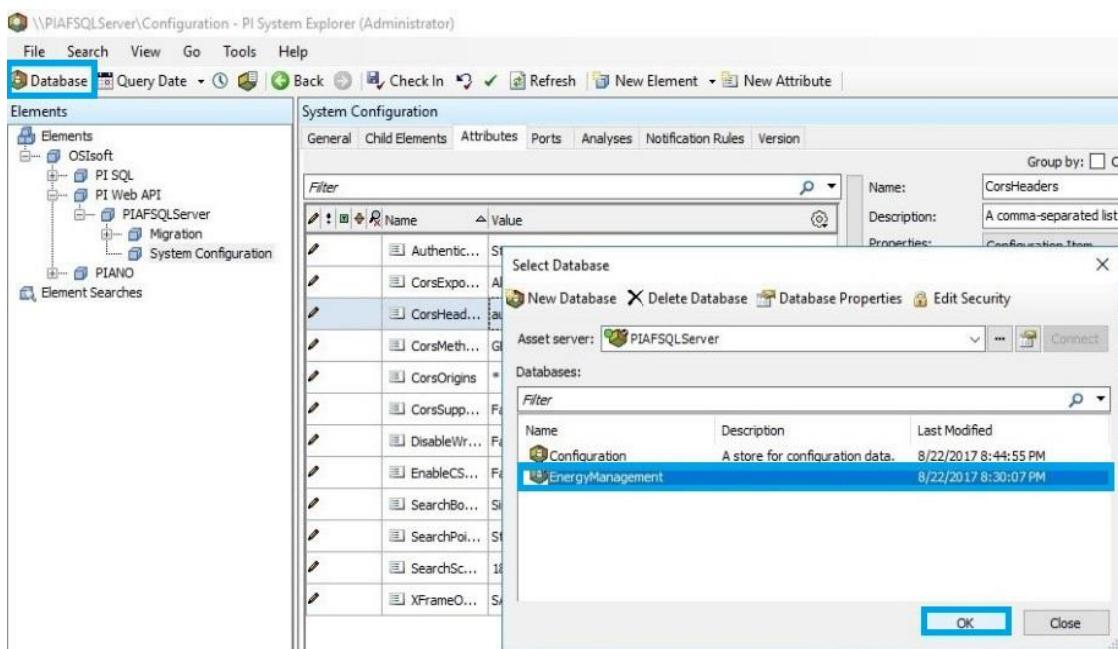


7. Select the **System Configuration** again and click on **Check In**.

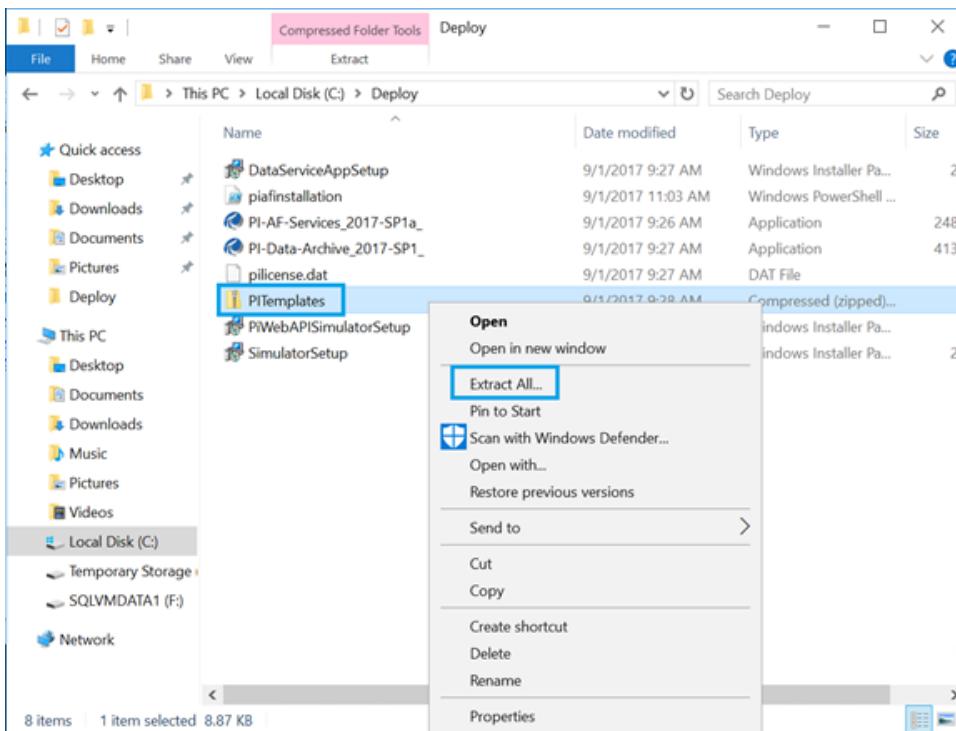


9.6. Import .XML Files into AF Server

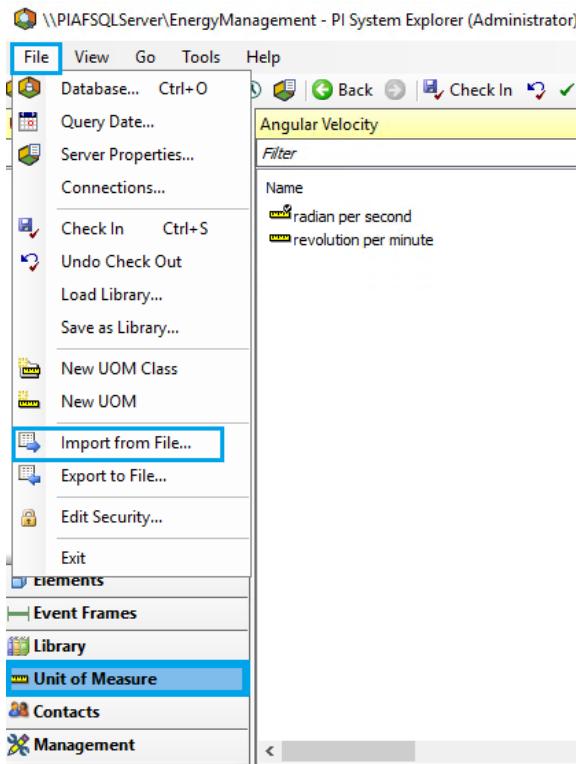
1. From the Bastion host connect to the **PIAFSQLServer** virtual machine through the private address with the credentials provided in the output section.
2. Navigate to **PI System Explorer > Select Database > Click on Energy Management > Click on OK.**



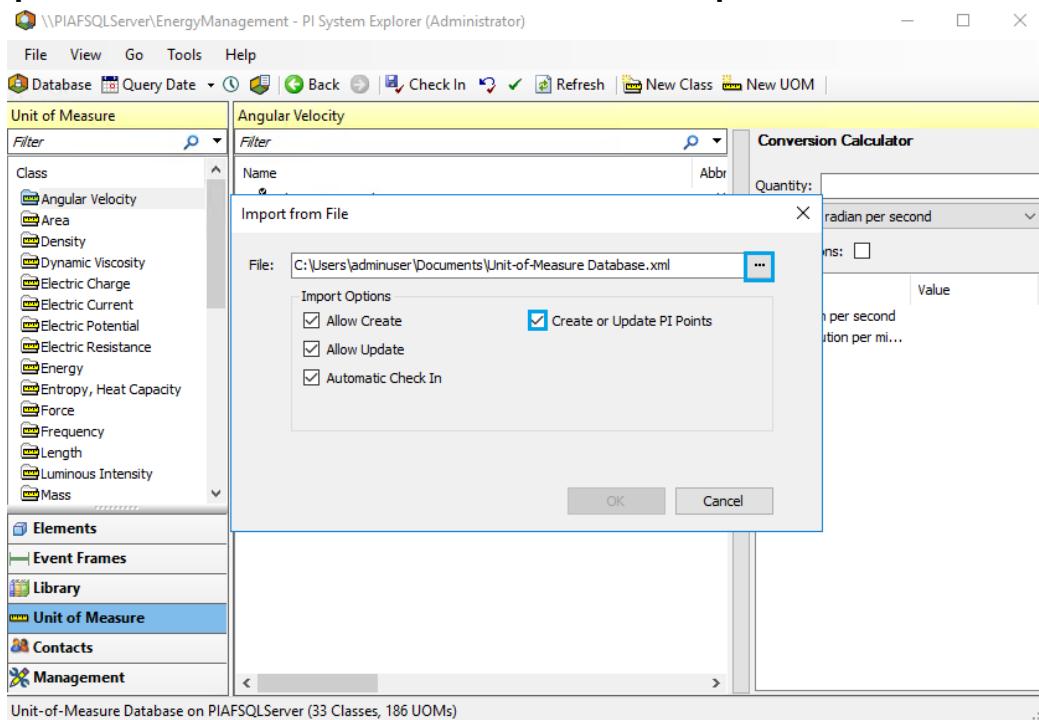
3. Navigate to Local disk (C:) > Deploy > unzip PI templates.



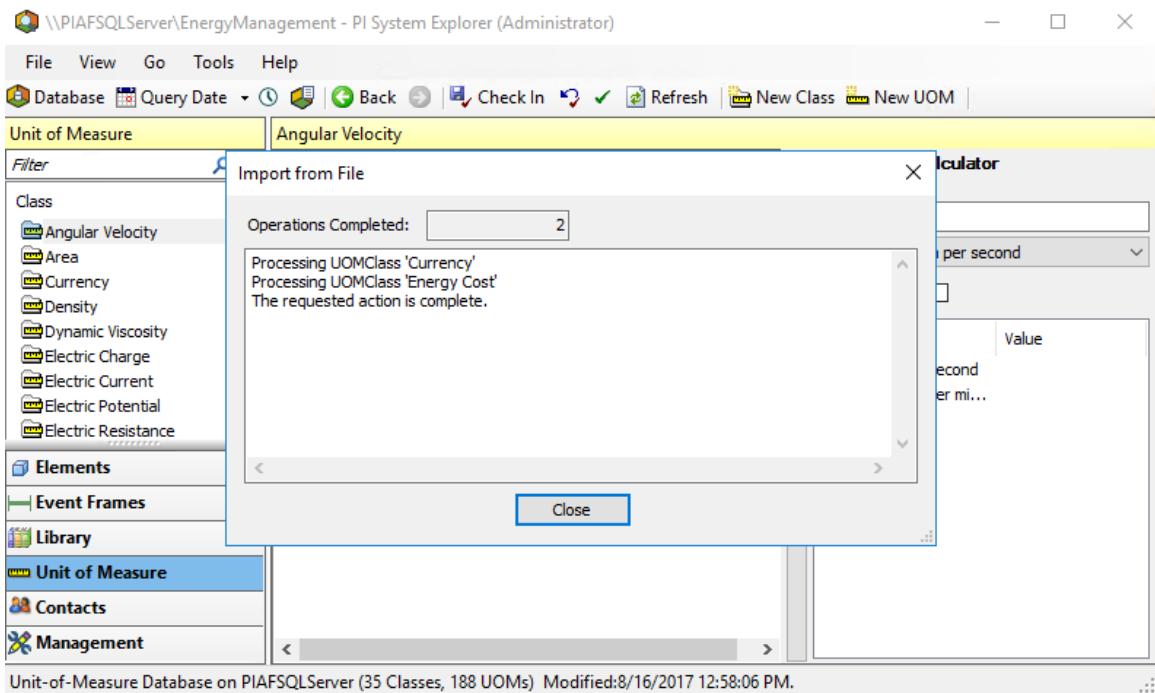
4. Select Unit of Measure > File > Import from file



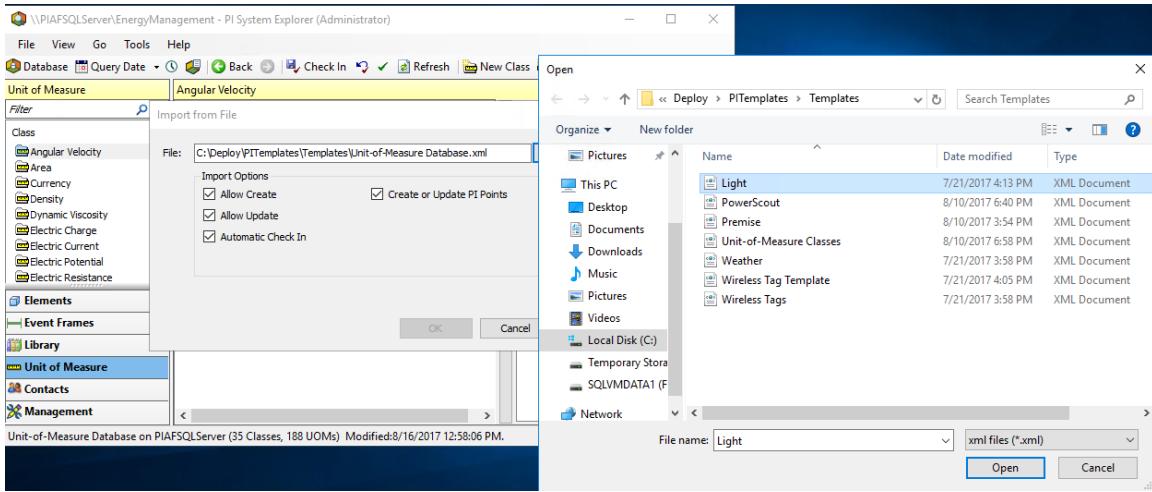
- Check the box for **Create or Update the PI Points** > browse to **local disk (C:)** > **Deploy** > **PITemplates** > Select **Unit of Measure Classes** > Click on **Open**.



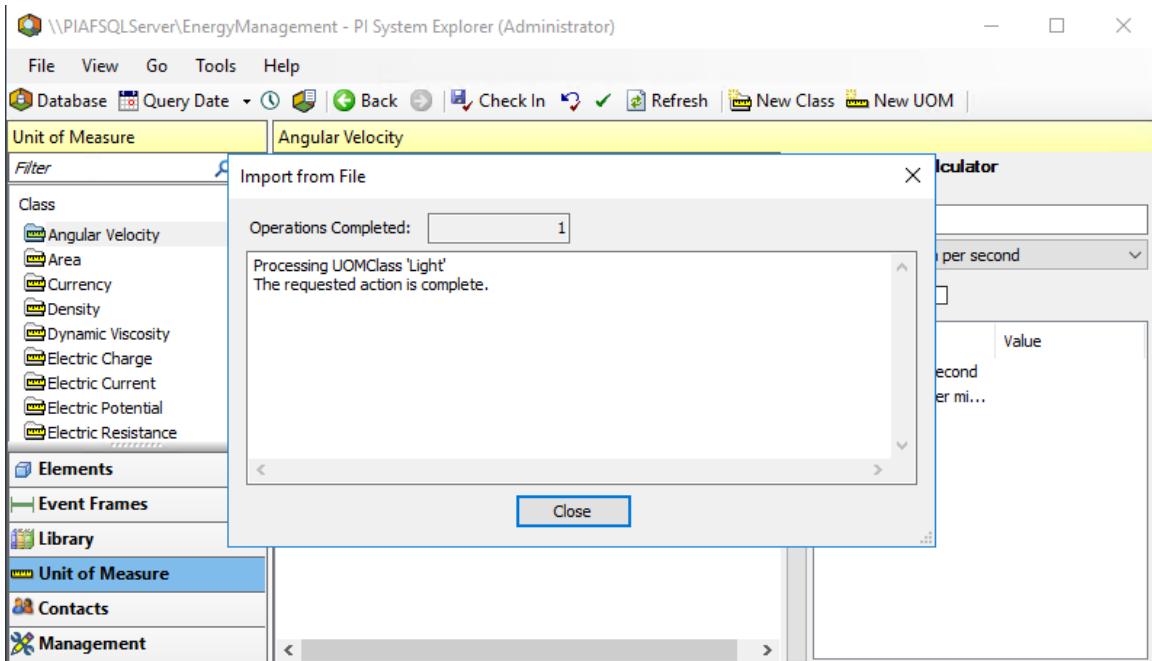
- You can find the status of the completed operation. Click on **Close**.



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

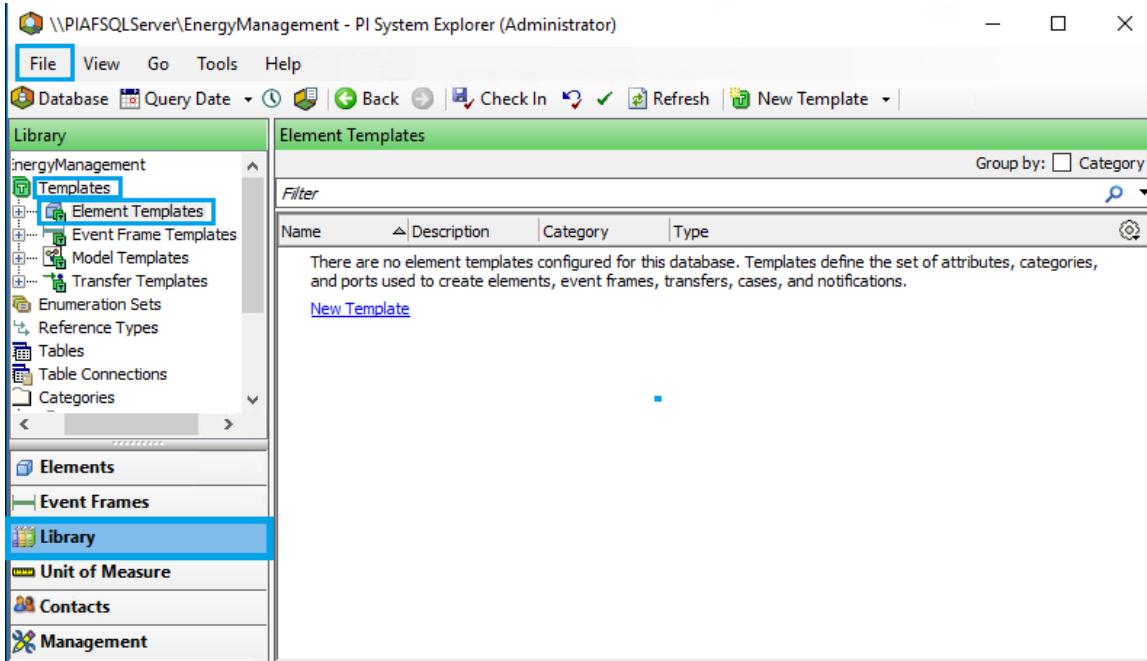


8. You can see the status of the completed operations. Click on **Close**.



9. Similarly Select **Library > Templates > Element Templates**. Click on **File > Import from file** (File location – C:\Deploy\PITemplates\Templates).

- Powerscout
- Wireless Tag Template



10. Similarly Select **Elements > Import File** (File location – C:\Deploy\PITemplates\Templates).

- 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

Group by: Category Template

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

Elements

Event Frames

Library

Unit of Measure

Contacts

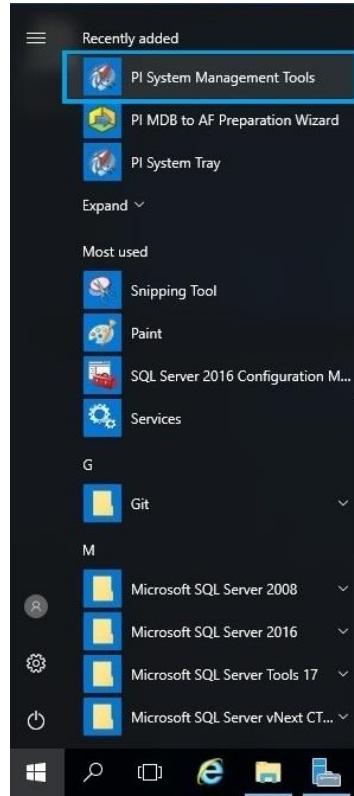
Management

3 Elements

The screenshot shows the PI System Explorer interface. The left sidebar contains a tree view under 'Elements' with nodes for Premise, Weather, and Wireless Tags. Below the tree is a list of categories: Event Frames, Library, Unit of Measure, Contacts, and Management. A status bar at the bottom indicates '3 Elements'. The main pane displays a search results grid titled 'Search' with columns for Name, Description, Category, Type, and Template. Three items are listed: Premise, Weather, and Wireless T..., all categorized as 'None' and typed as 'None'. A search bar at the top right is labeled 'Search Elements'.

9.7. Update Security in PI System Management Tools

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



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



Customer Experience Improvement Program

X



Do you want to participate in the PI System Management Tools Customer Experience Improvement Program?

This software includes a usage reporting capability that enables OSIsoft to collect anonymous data about the use of its features. You can help us improve our products by allowing your usage data to be sent to OSIsoft.

The data we collect includes no identifiable information that could be used to trace back to a particular user or computer, and no business data or logic is collected. We aggregate data from all participants to develop usage statistics that will help us improve our software and service and prioritize the development of new features. You can end your participation in usage data collection at any time via the Help/Customer Feedback Option in PI System Management Tools.

Yes, I want to participate in the program (recommended)

No, I do not want to participate in the program

OK

Cancel

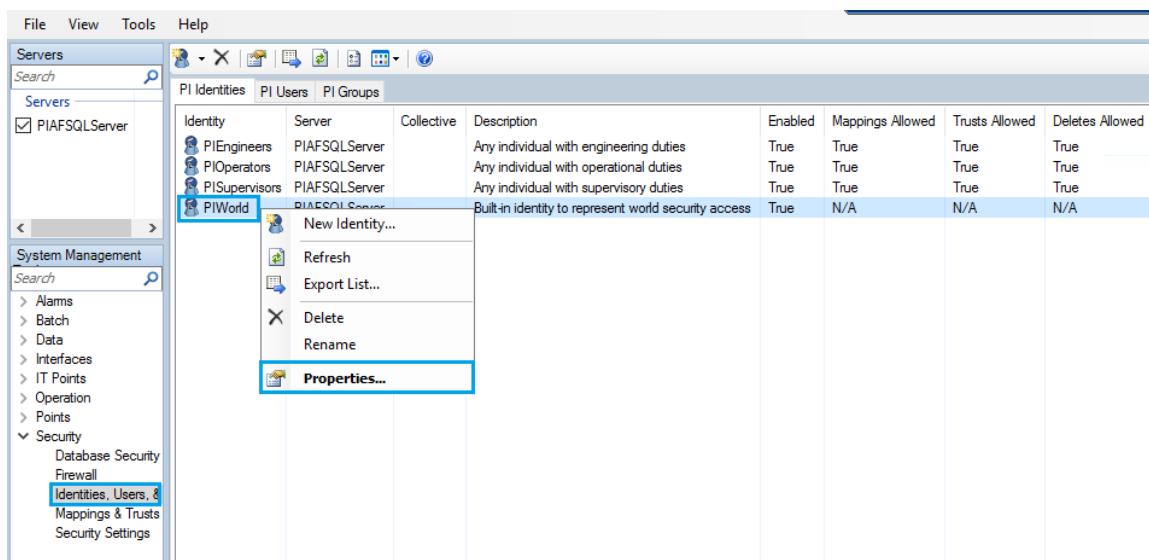
3. Under Servers, check the **PIAFSQLServer** box.

The screenshot shows the PI System Management Tools (Administrator) window. The menu bar includes File, View, Tools, and Help. Below the menu is a 'Servers' list with a search bar. A checkbox next to 'PIAFSQLServer' is checked. To the right of the servers list are two icons: 'Alarm Groups' and 'SQC Alarms'.

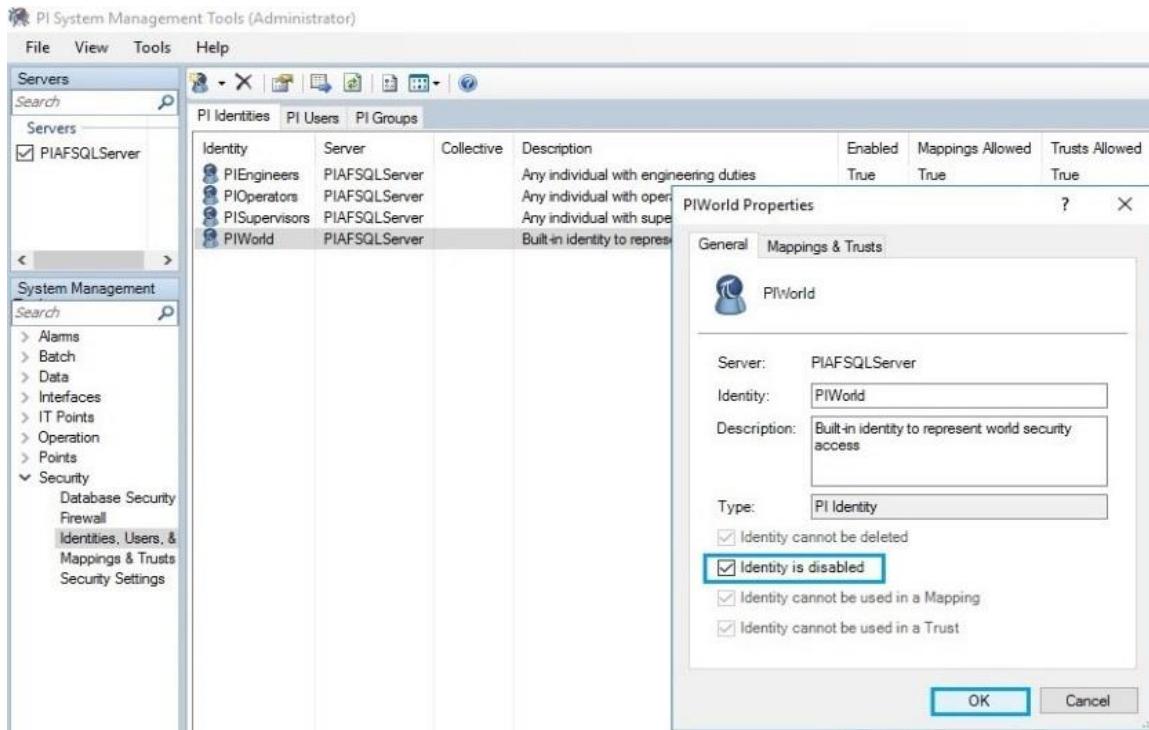
4. Click on **Security** under **System Management**, then click on **Security Settings**.



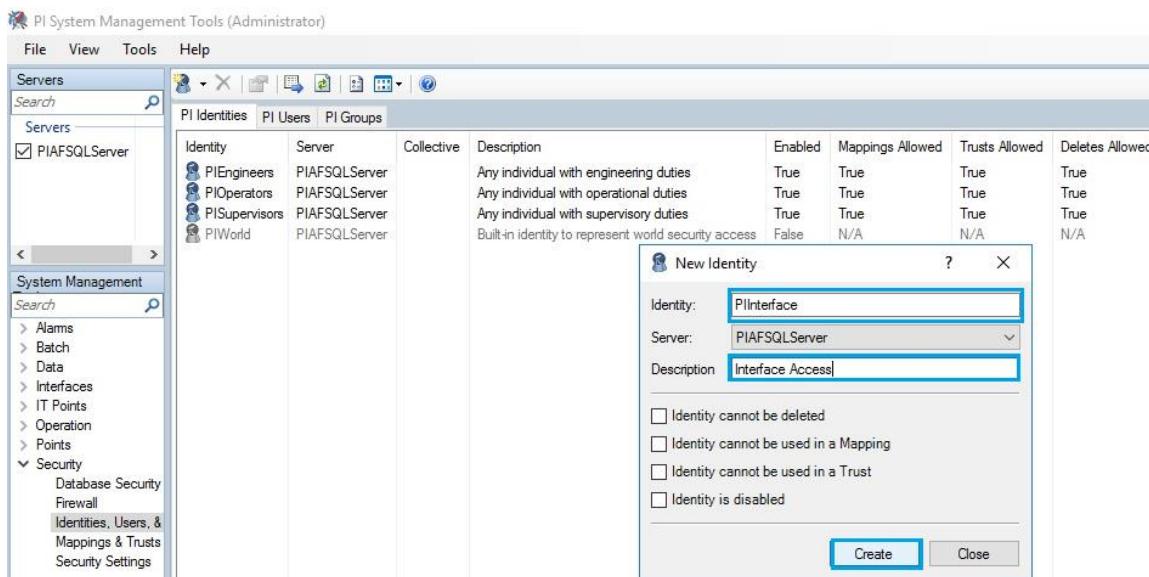
5. Click on **Identities, Users and Groups**, then right-click on **PIWorld** under PI identities and select **Properties**.



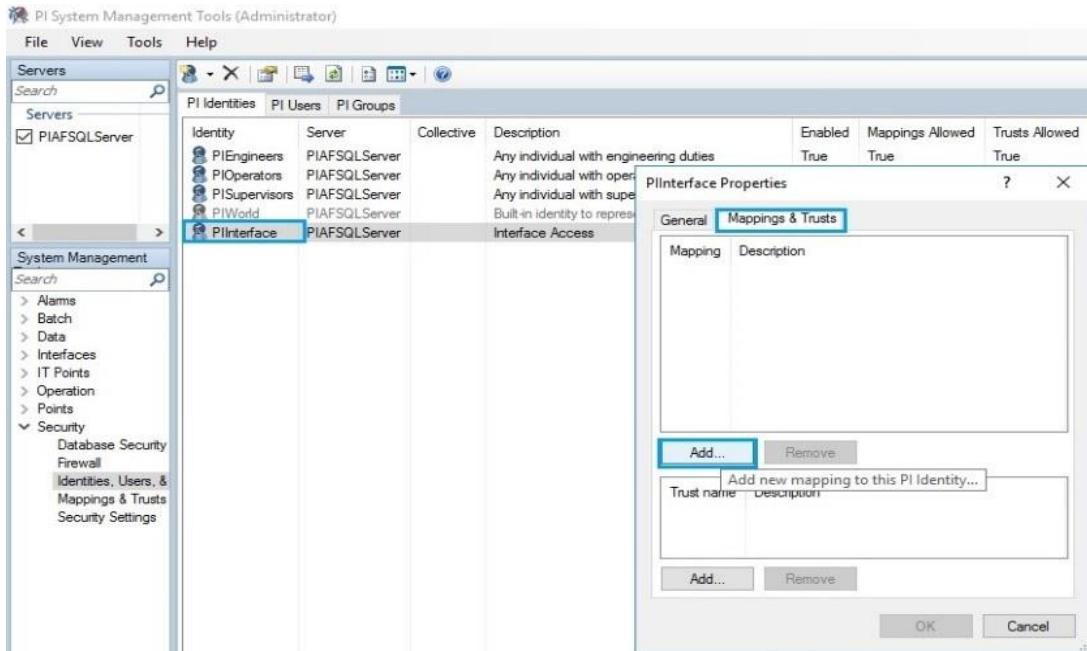
- Select the **Identity is disabled** checkbox and click on **OK**.



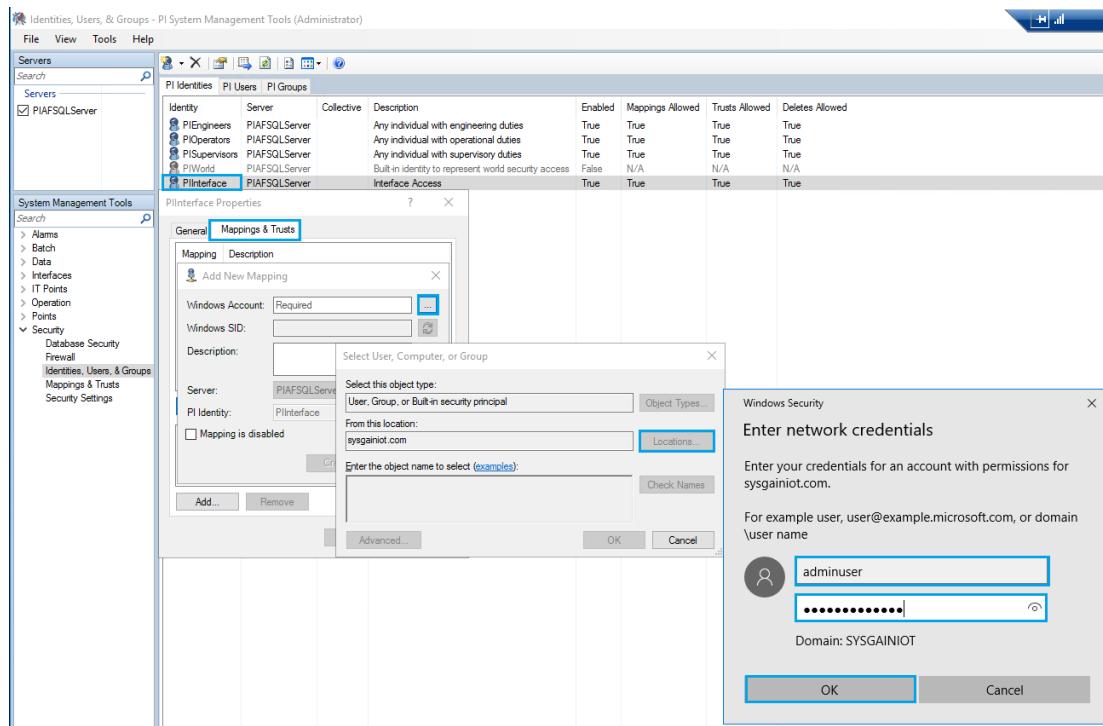
- The **Enabled** column under **PIWorld** will appear as **False**.
- Right-click **PI Identities** to create a new identity. Give the identity the name **PIInterface** and the description **Interface Access**, then click on **Create**.



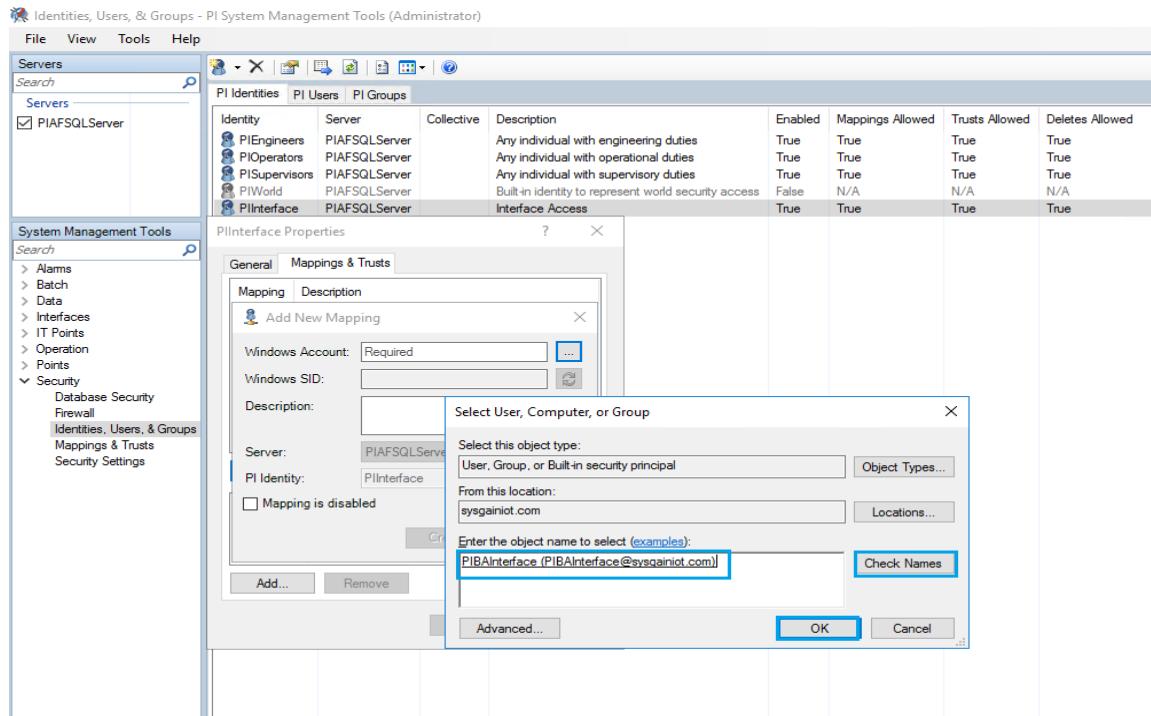
9. Right-click on the newly created **PIInterface** identity, then go to **Properties > Mappings & Trusts**, then click on **Add**.



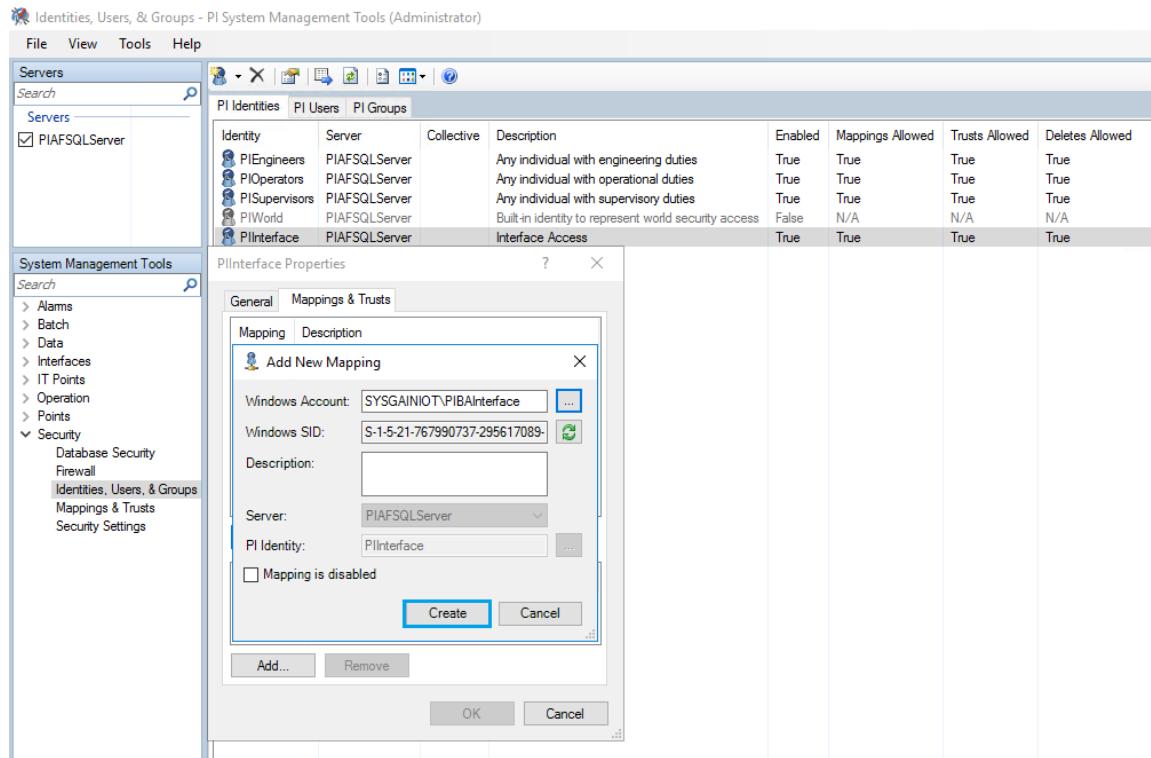
10. After click on **Add** it will show the popup box Add new mapping in that **Browse** at end of **Windows Account** again it will show the popup box as select user,computer,or group in that click on **Locations**. select the domainname Enter the credentials and click on **OK**



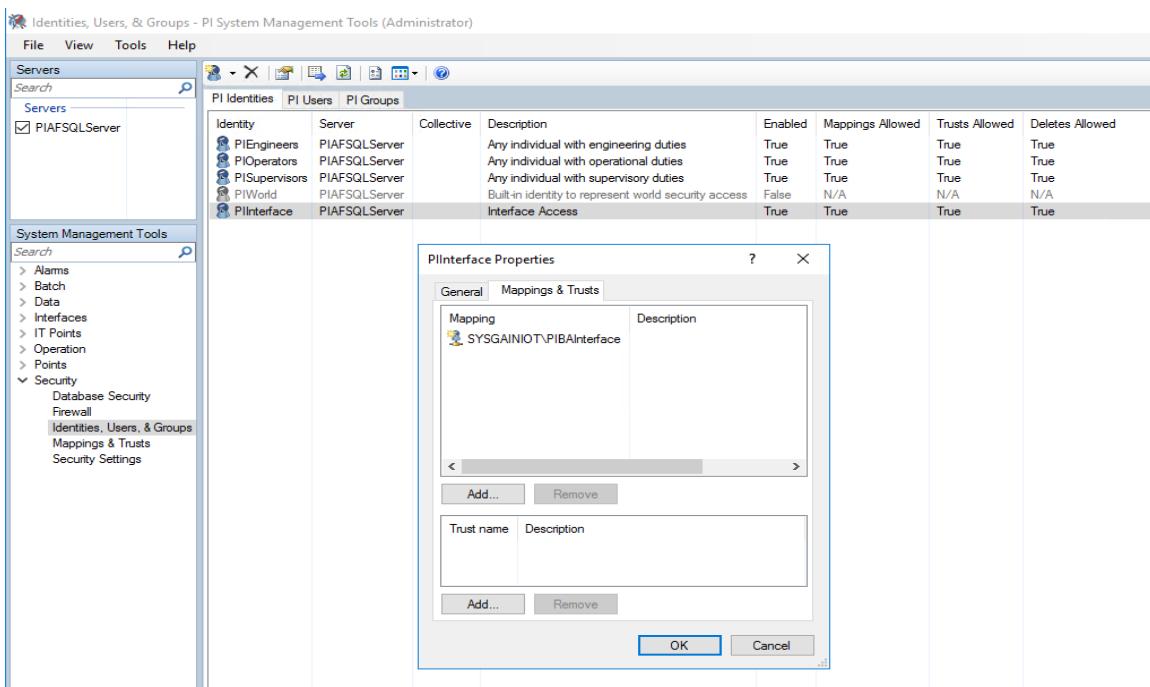
11. Give object name as **PIBAInterface** > Click on **Check Names** > **OK**



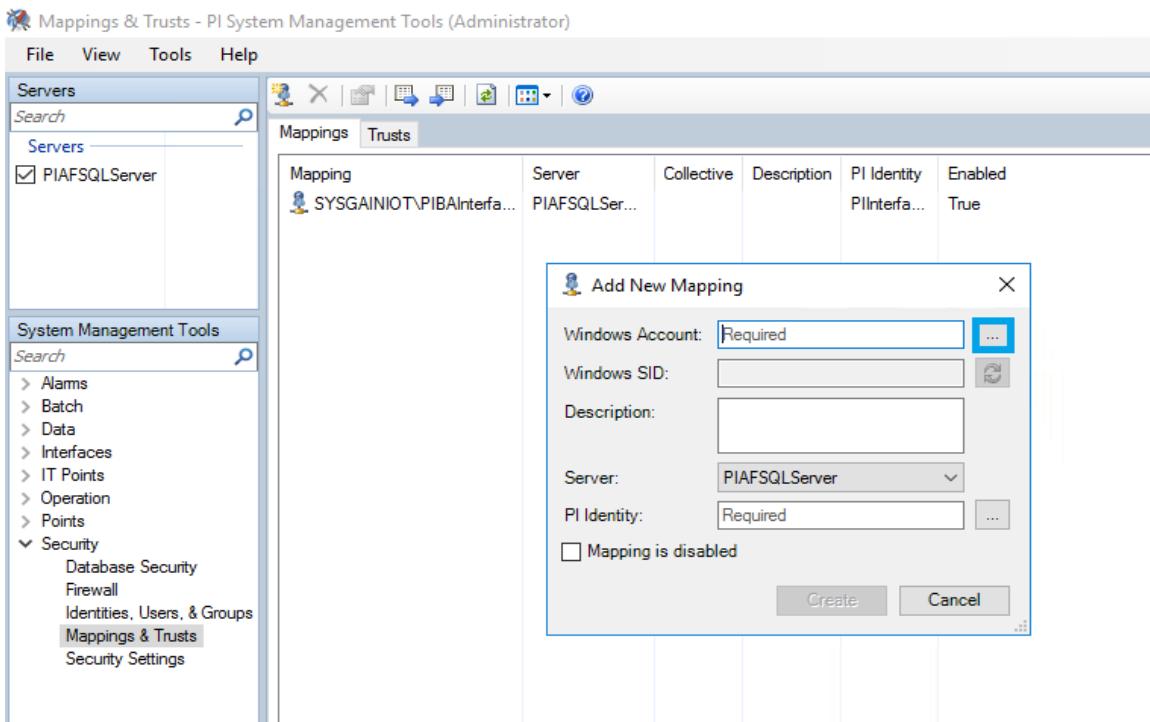
12. Click on **Create** to create a New Mapping for PIBAInterface.



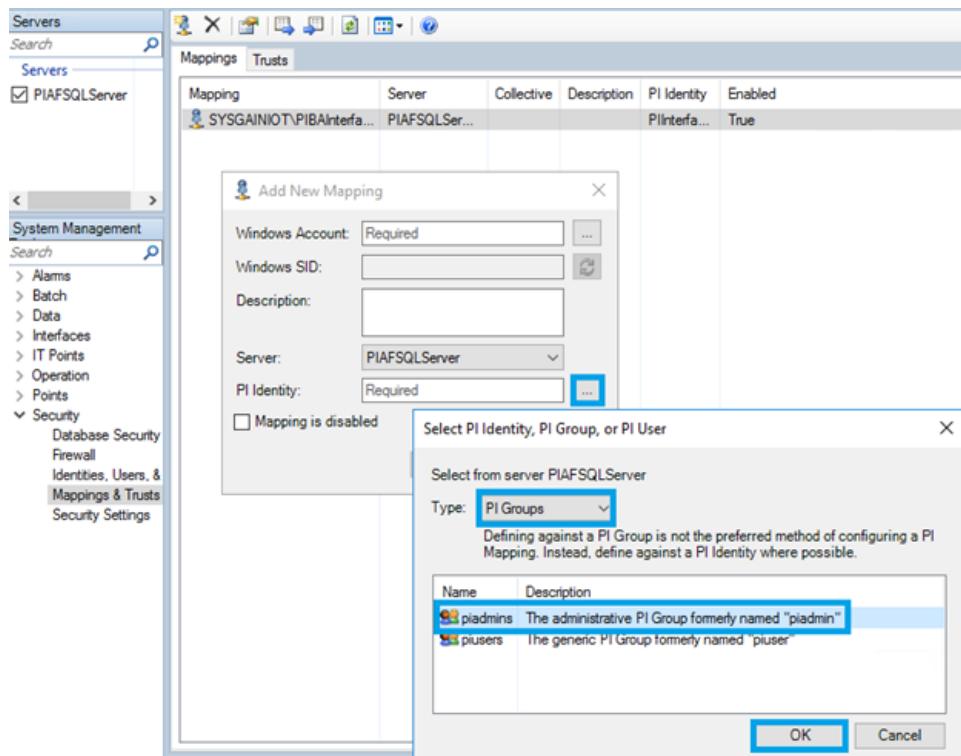
13. Click **OK** once the PIBAInterface mapping is created.



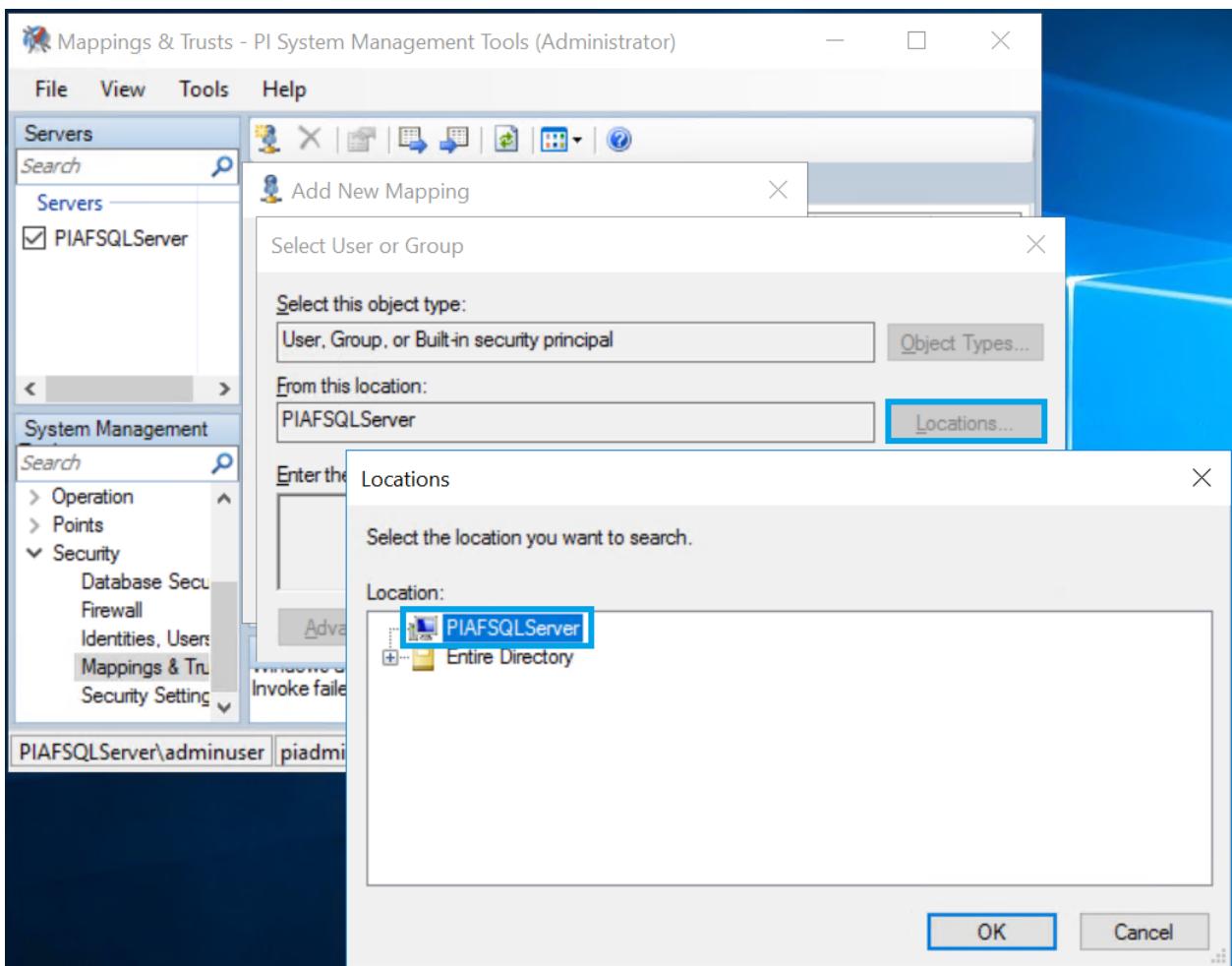
14. Navigate to **Security > Mapping & Trusts** to create a New Mapping.



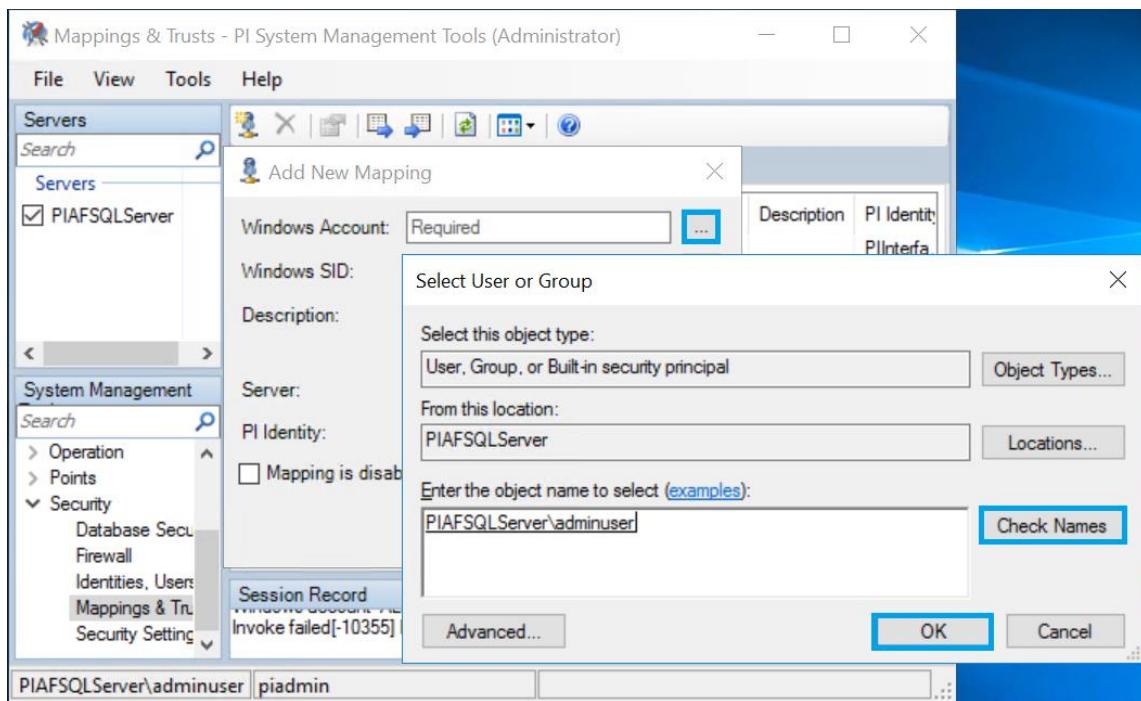
15. Browse the directory in **PI Identity** section, then select **PI groups** under the **Type** dropdown and Select **piadmins** to create PI Identity as **piadmins**.



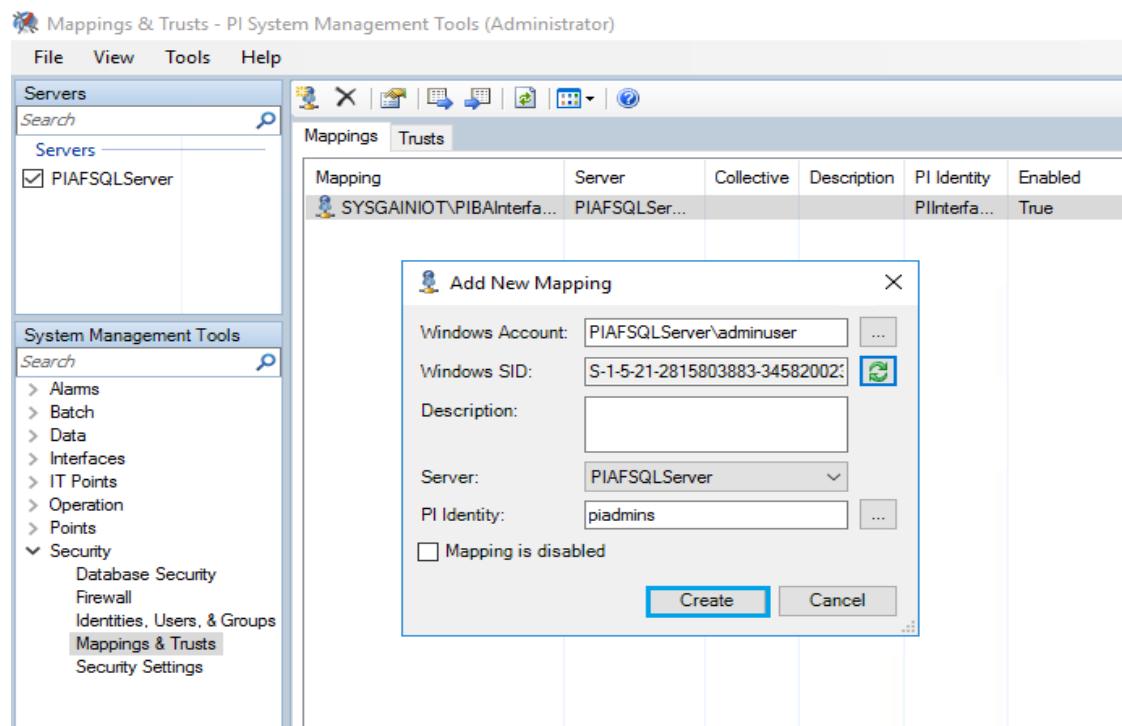
16. Click the dots next to **Windows Account**, then **Locations**, and select the **PIAFSQLServer**. Click on **OK**.



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

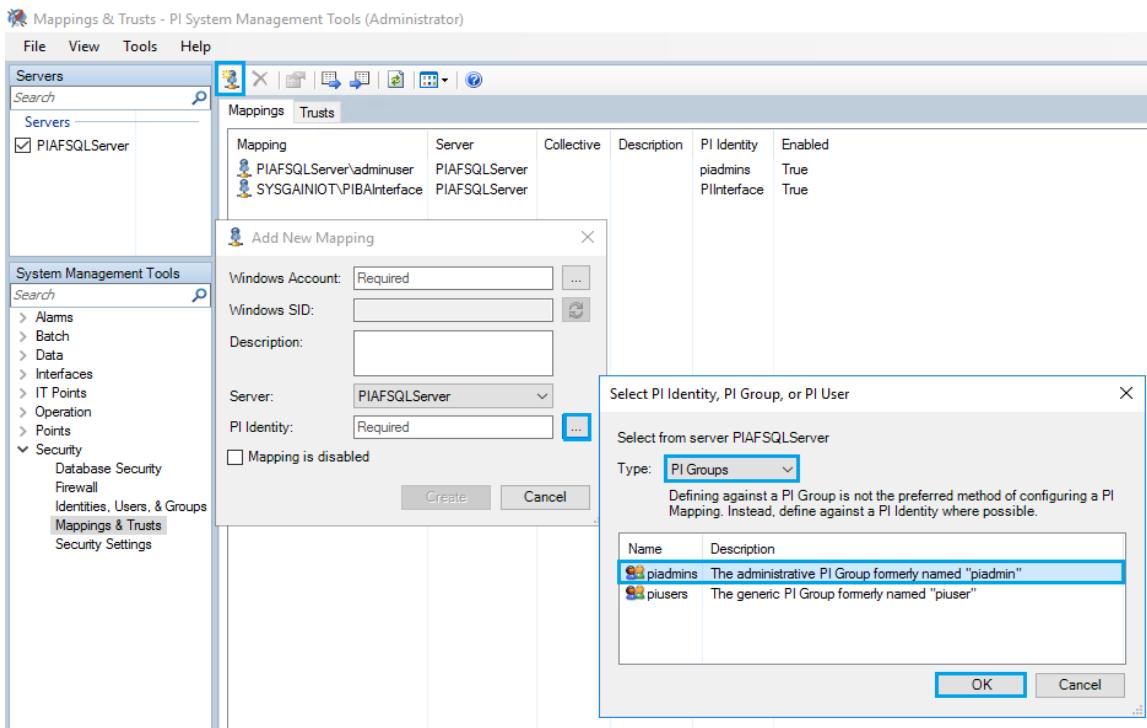


18. Click **Create** on **on**

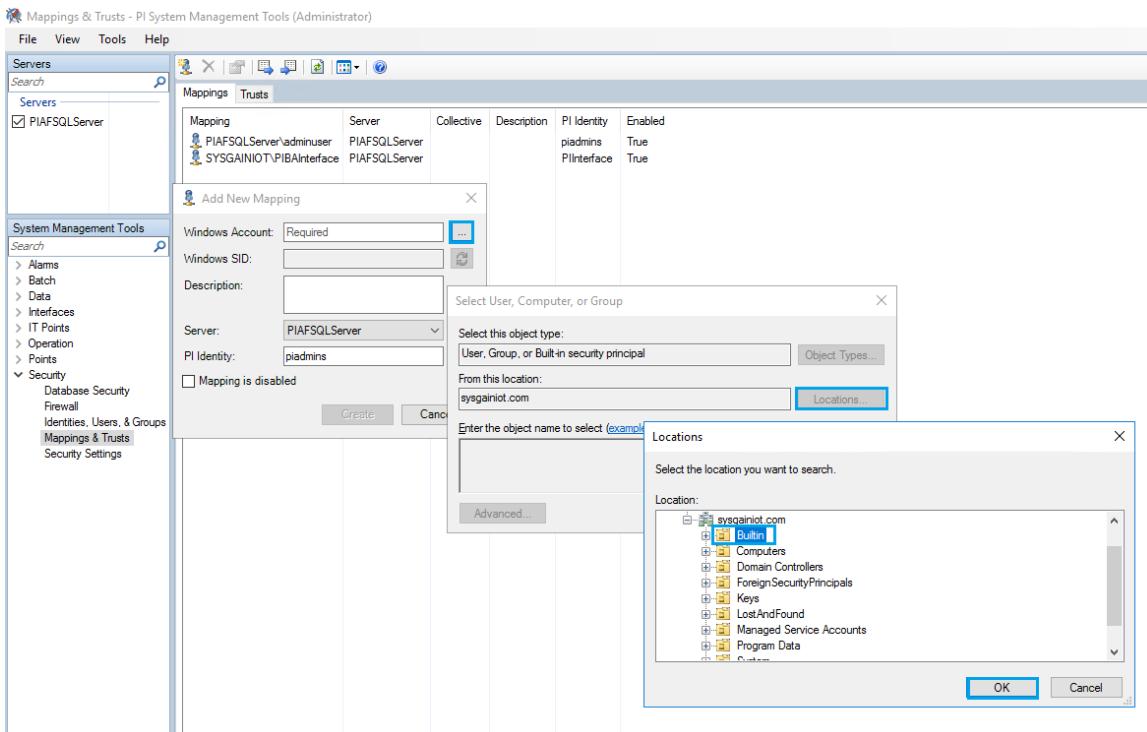


19. Create a new Mapping for **Administrator**.

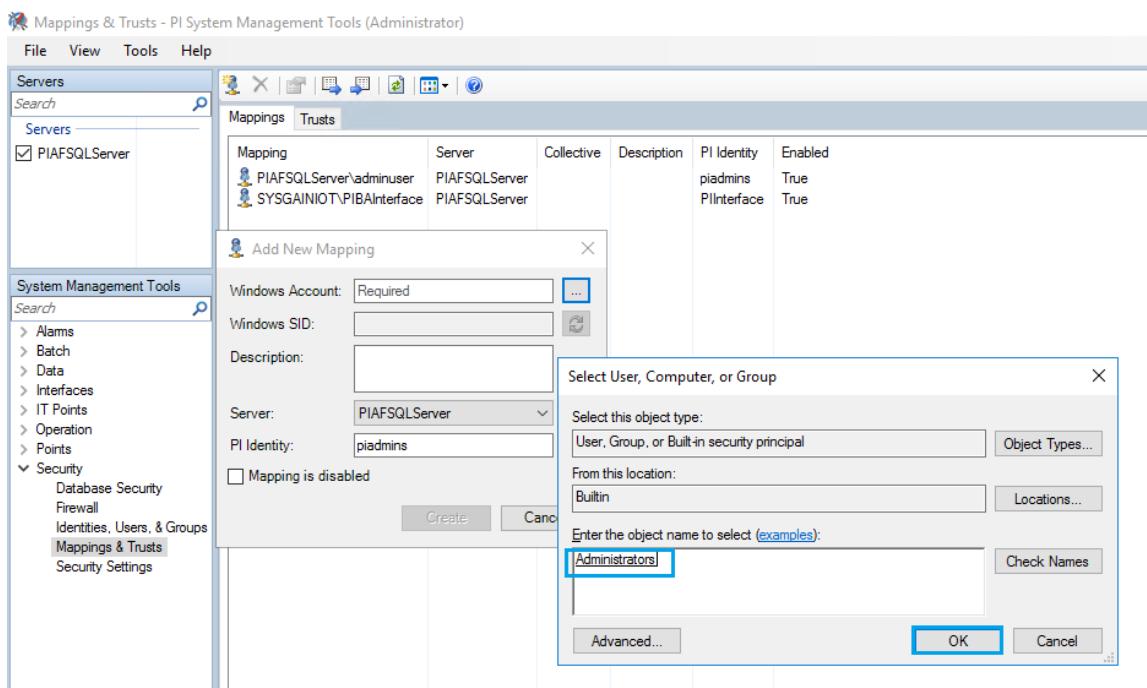
20. Near **PI Identity**, select **Type as PI Groups** > Select **piadmins** > Click on **OK**.



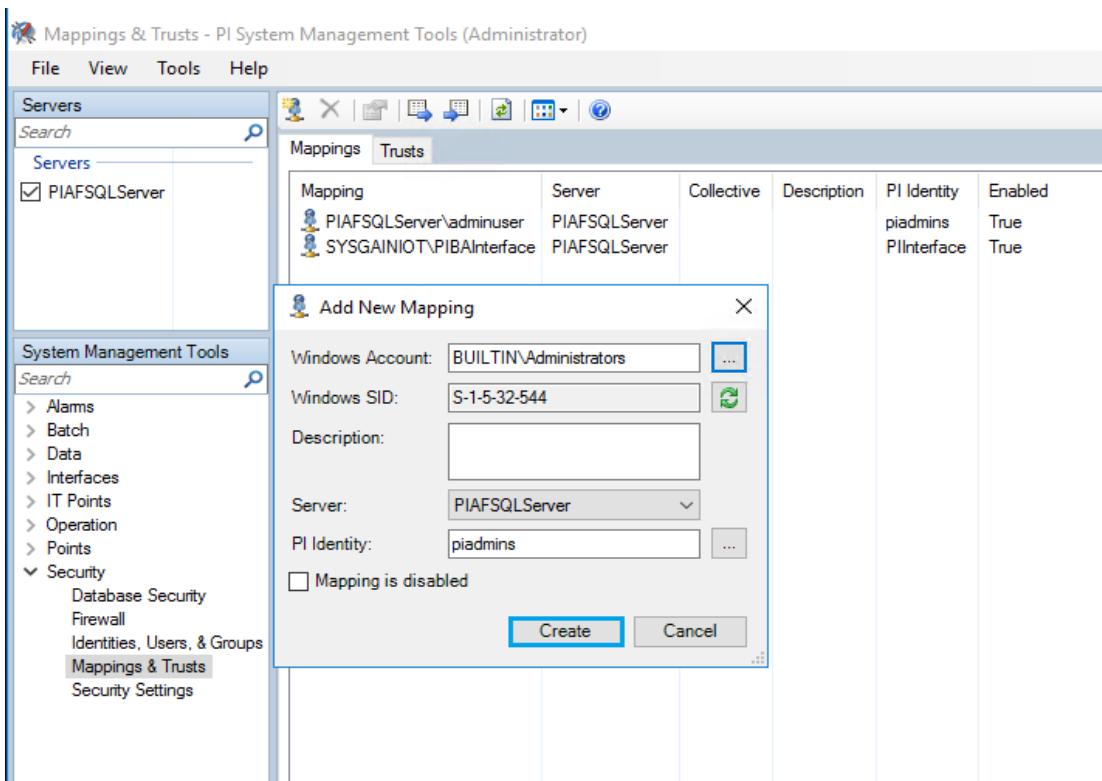
- Click the Browse dots near **Windows Account** > Select **Locations** > click on **sysgaiiot.com** > Select **Builtin** > Click **OK**.



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.

The screenshot shows the 'Mappings & Trusts' interface in the PI System Management Tools. The left sidebar shows 'Servers' with 'PIAFSQLServer' selected. The main pane shows a table of 'Mappings' with the following data:

Mapping	Server	Collective	Description	PI Identity	Enabled
BUILTIN\Administrators	PIAFSQLServer			piadmins	True
PIAFSQLServer\adminuser	PIAFSQLServer			piadmins	True
SYSGAINIOT\PIBAInterface	PIAFSQLServer			PIInterface	True

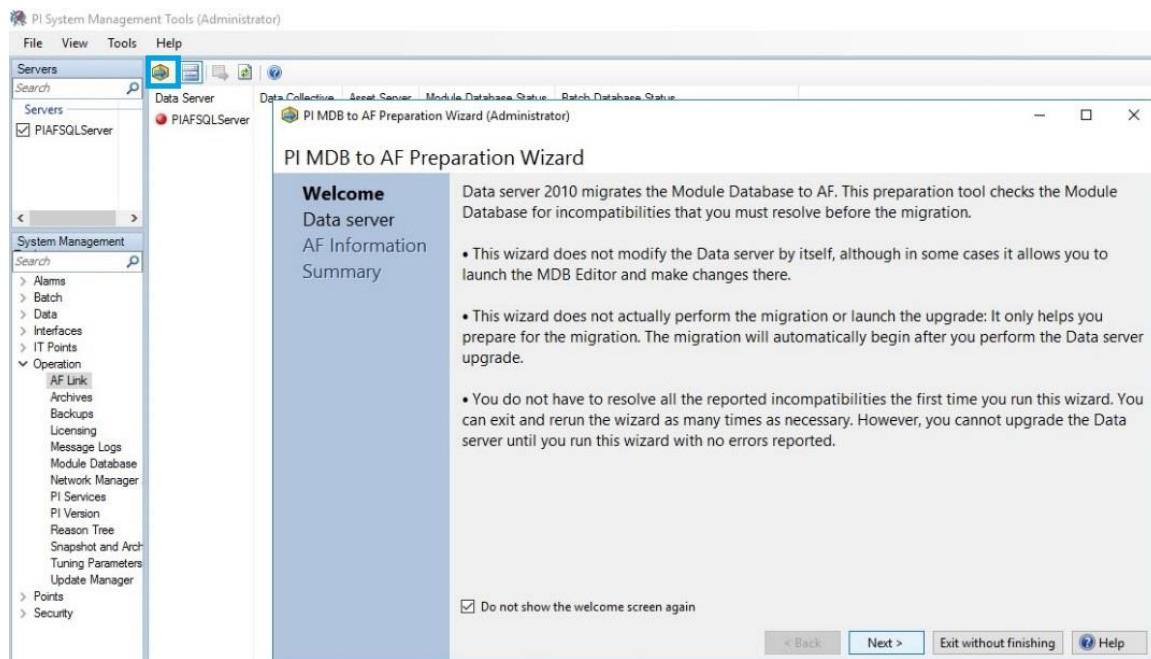
The 'System Management Tools' sidebar on the left is expanded, showing the 'Security' section with 'Mappings & Trusts' selected.

9.8. Prepare Data Server For Module Database(Mdb) To Asset Framework(AF)

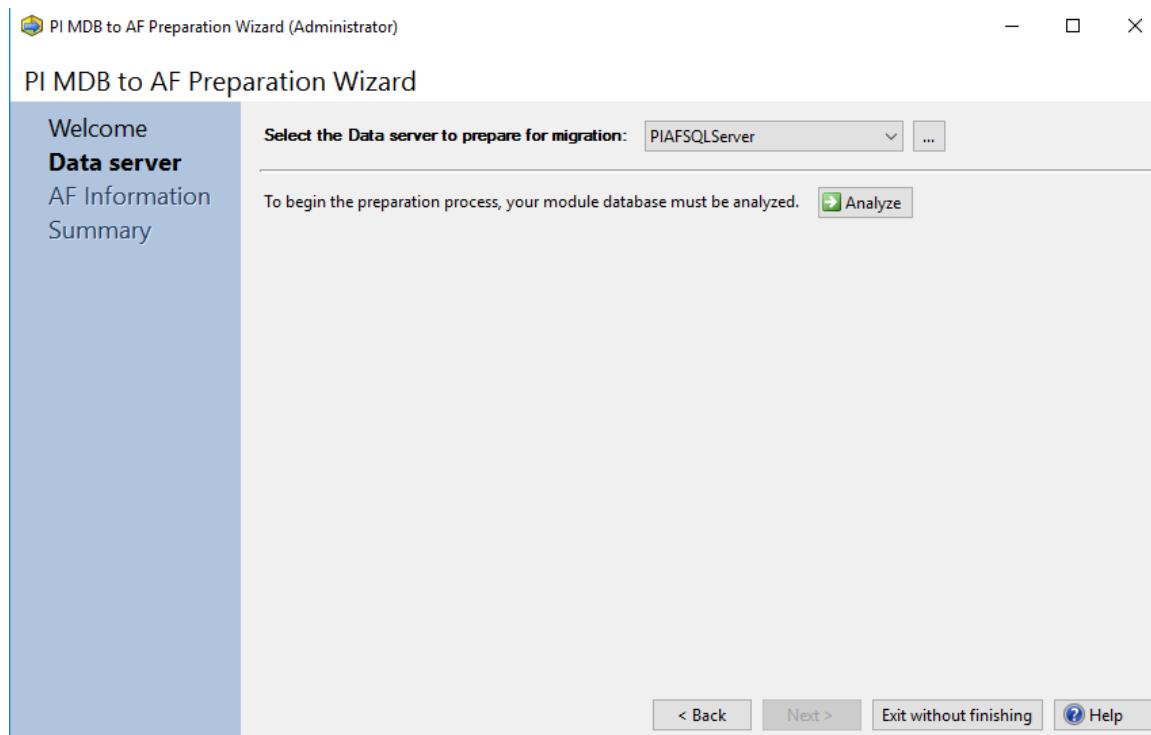
1. Navigate to **PI System Management Tools > Operation > Click on AF link.**

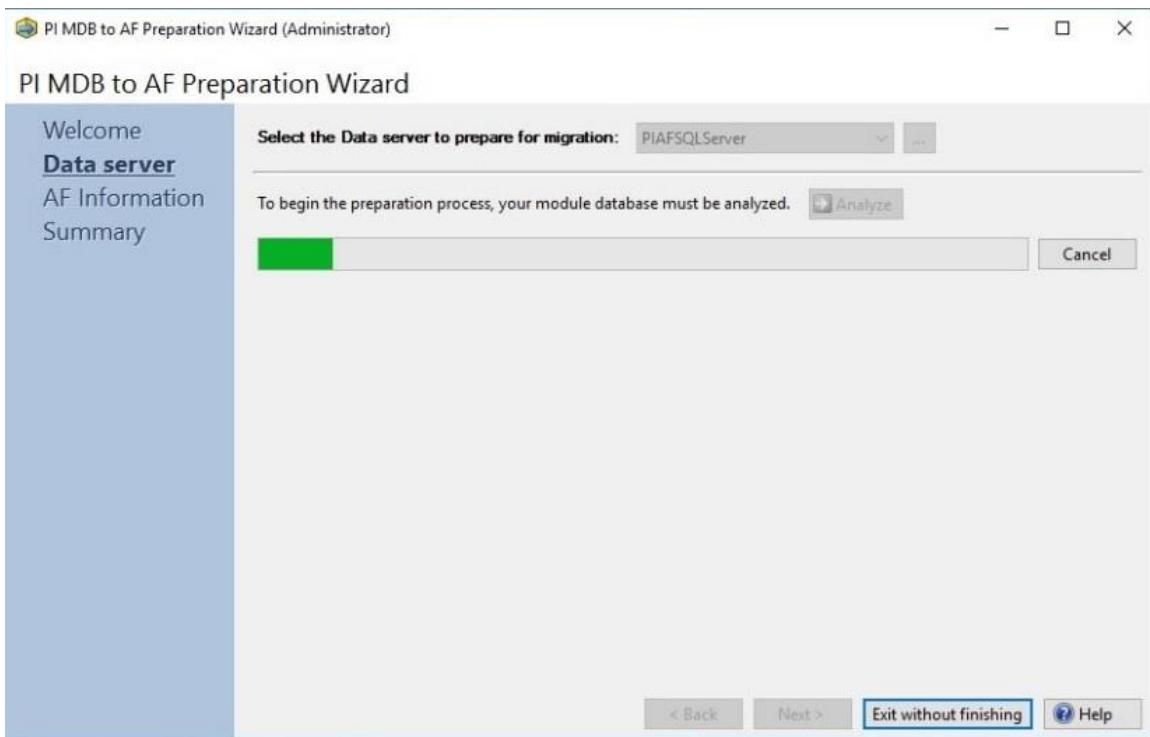
The screenshot shows the 'Operation' interface in the PI System Management Tools. The left sidebar shows 'System Management' with 'Operation' selected. The top navigation bar has 'AF Link' highlighted. The toolbar includes icons for AF Link, Archives, Backups, Licensing, Message Logs, Module Database, Network Manager, PI Services, PI Version, Reason Tree, Snapshot and Archive Sta..., Tuning Parameters, and Update Manager. The 'Servers' sidebar shows 'PIAFSQLServer' selected.

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. Click on **Next**.

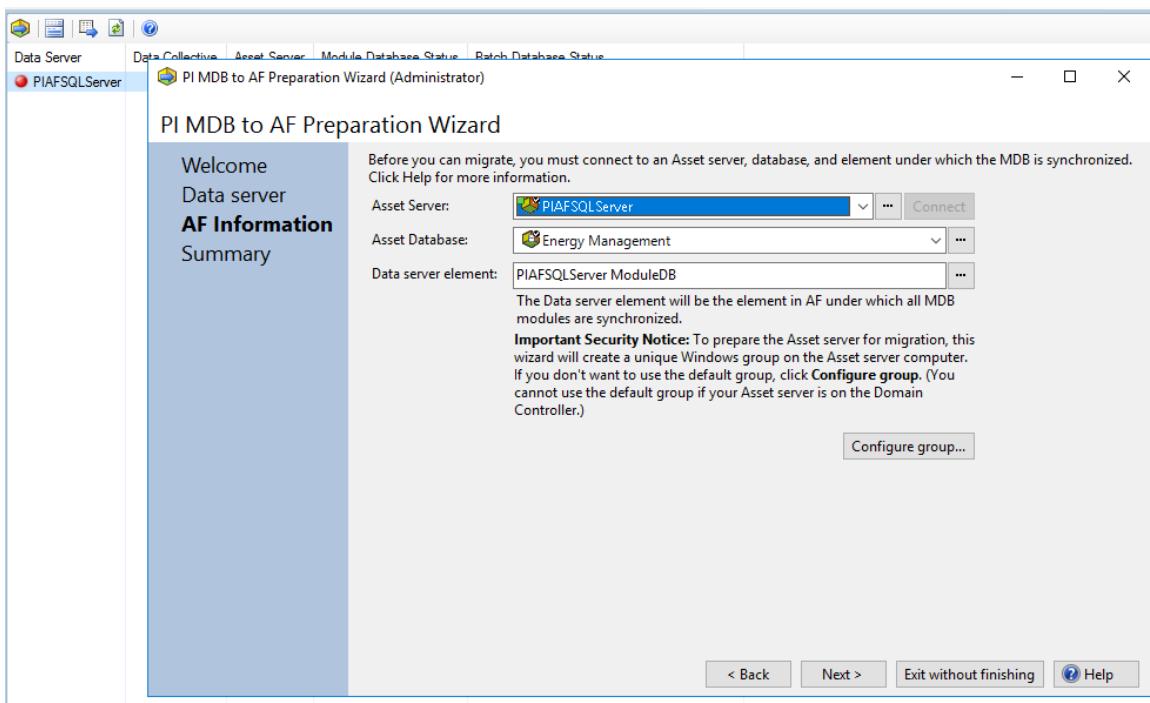


3. Click on **Analyze**, then click on **Next** once the process is complete.

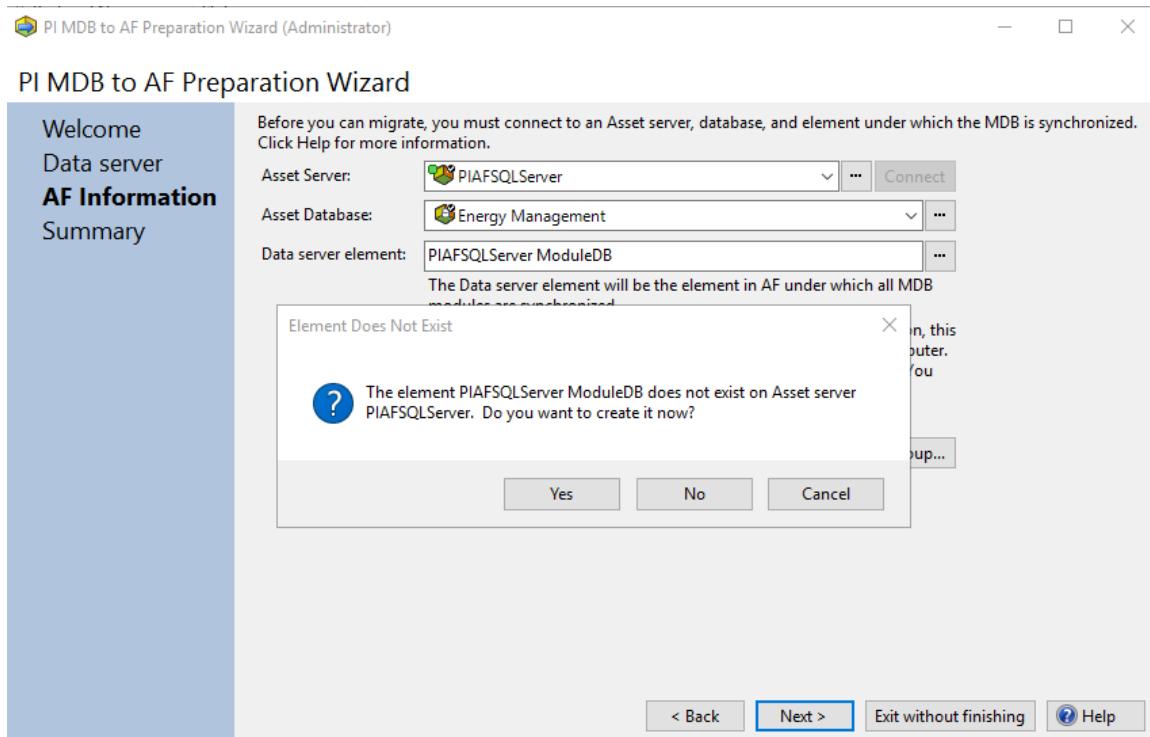




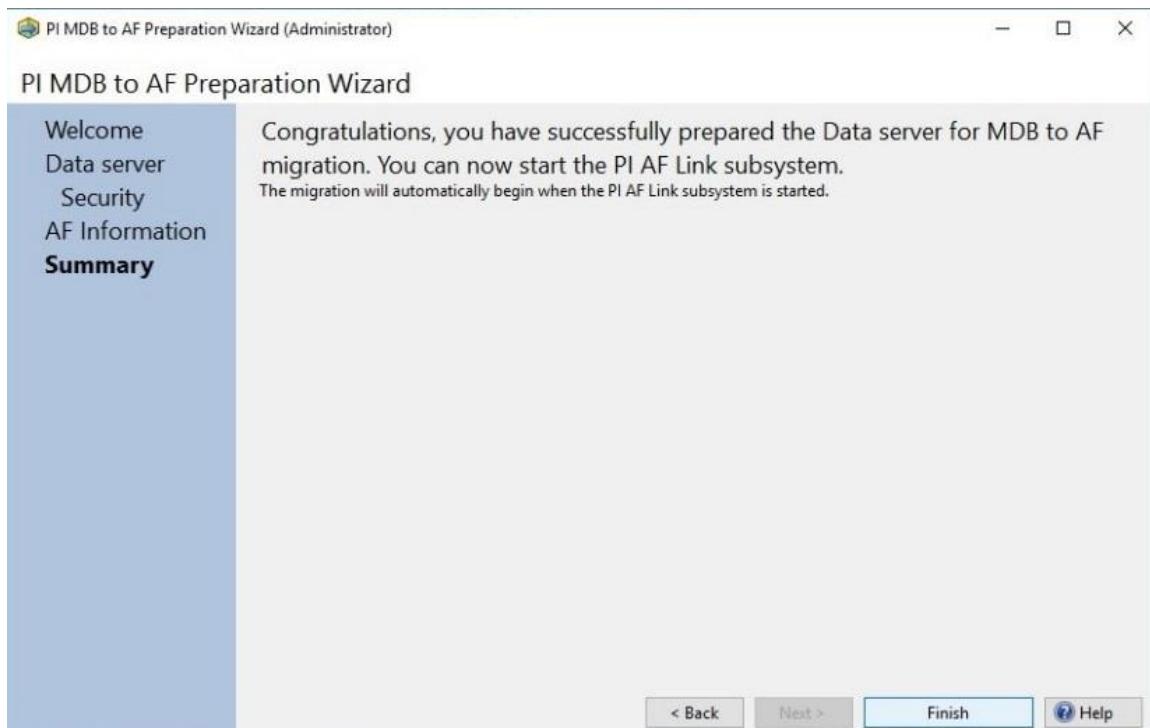
4. In AF Information, set the **Asset Server** as **PIAFSQLServer**, then click on **Connect**. Set **Asset Database** as **Energy Management**. Click on **Next**.

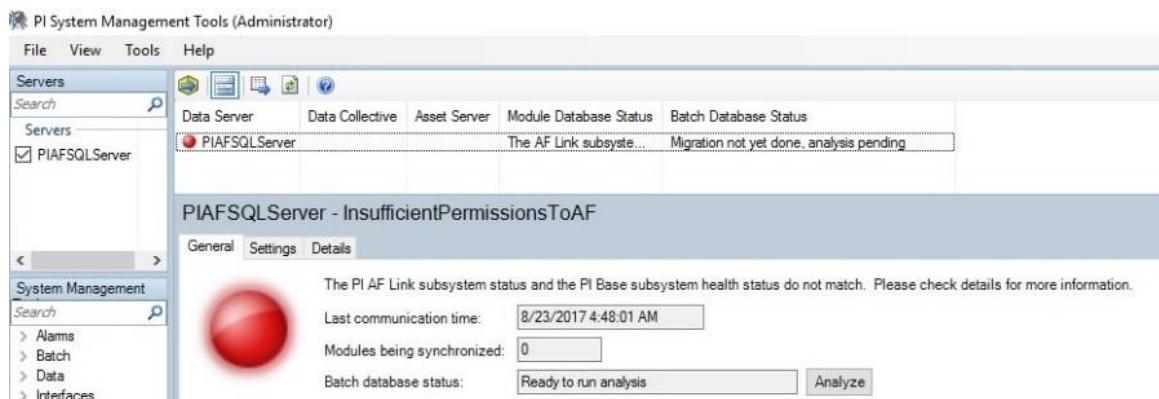


5. Click on **Yes** to create a PIAFSQLServer ModuleDB, then click on **Next**.

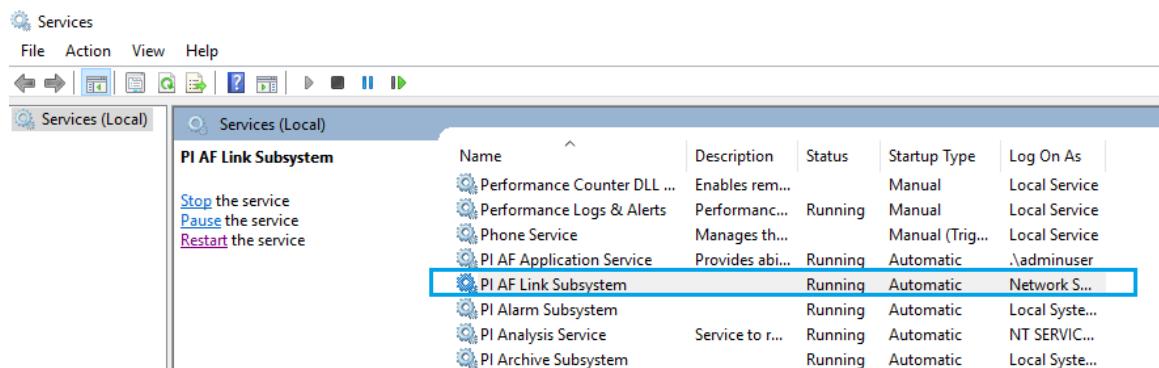


6. Click on **Finish**.

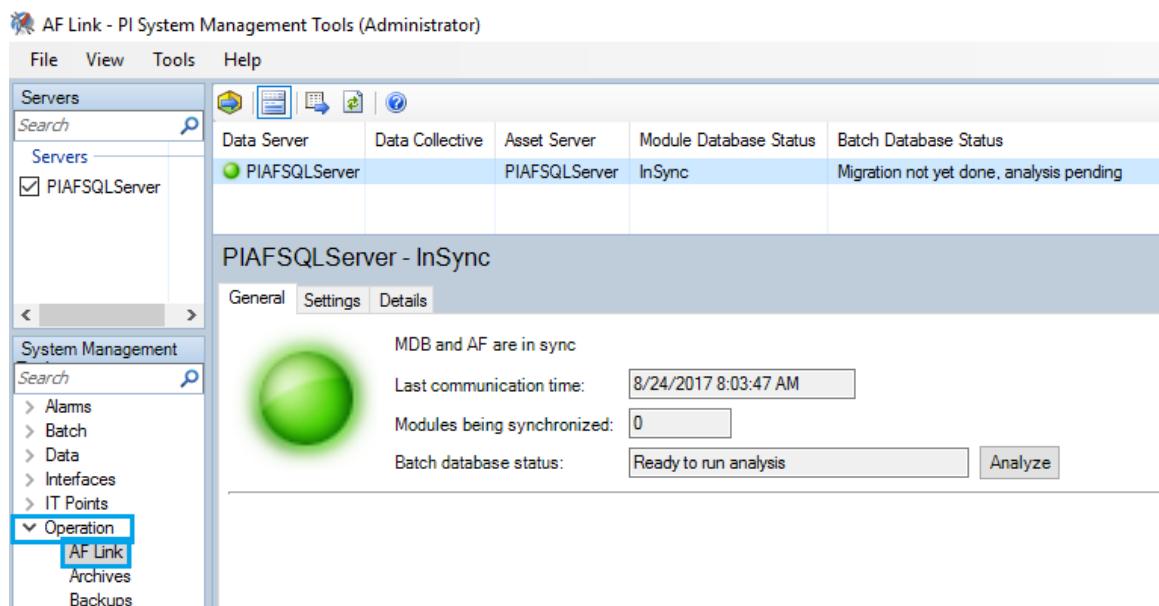




7. If you see the red circle on PIAFSQL Server, go to the **Services.msc** and restart the service **PI AF Link Subsystem**.



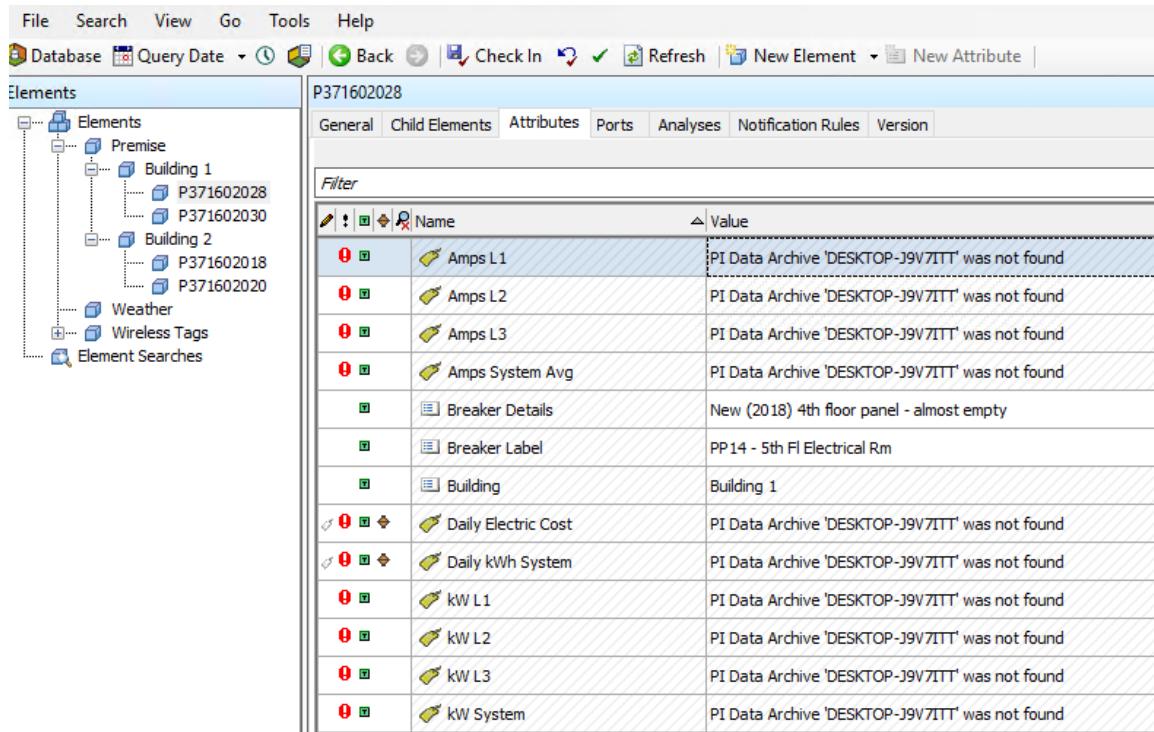
8. After restart, go to the **Operations** under system management and click on **AF Link**. You can see the PIAFSQL Server now has a green circle.



9.9. Update PI Points in PI System Explorer

1. Open **PI System Explorer** from the Start Menu in the PI System folder.
2. Navigate to **Elements > Premise > Click on Building1, Building2 > Click on Attributes.**

You will notice a red symbol next to some of the attributes. These Attributes must be updated.



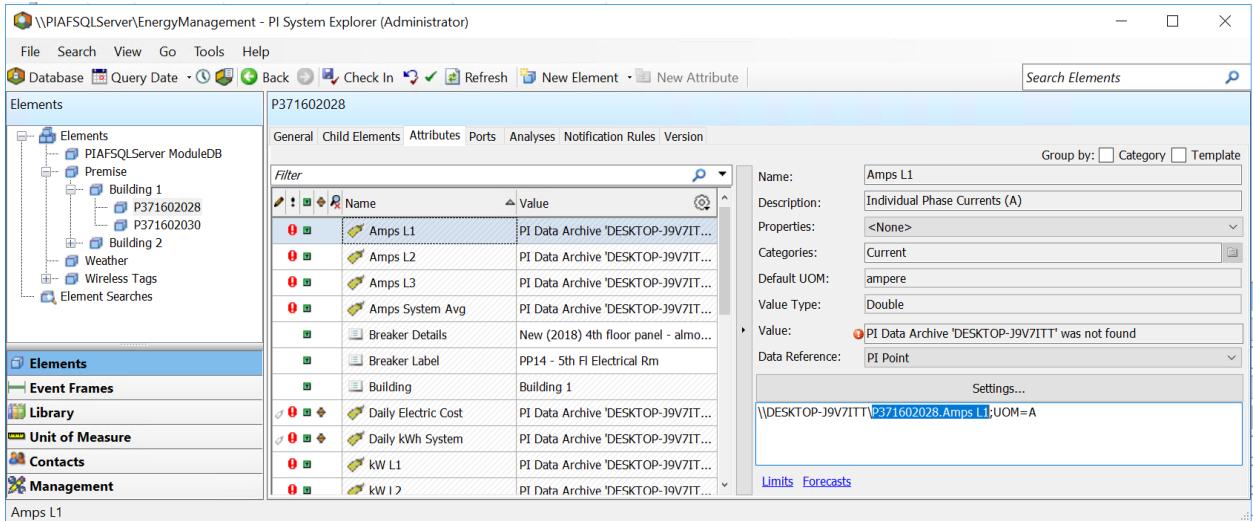
Name	Value
Amps L1	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L2	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps L3	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Amps System Avg	PI Data Archive 'DESKTOP-J9V7ITT' was not found
Breaker Details	New (2018) 4th floor panel - almost empty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

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

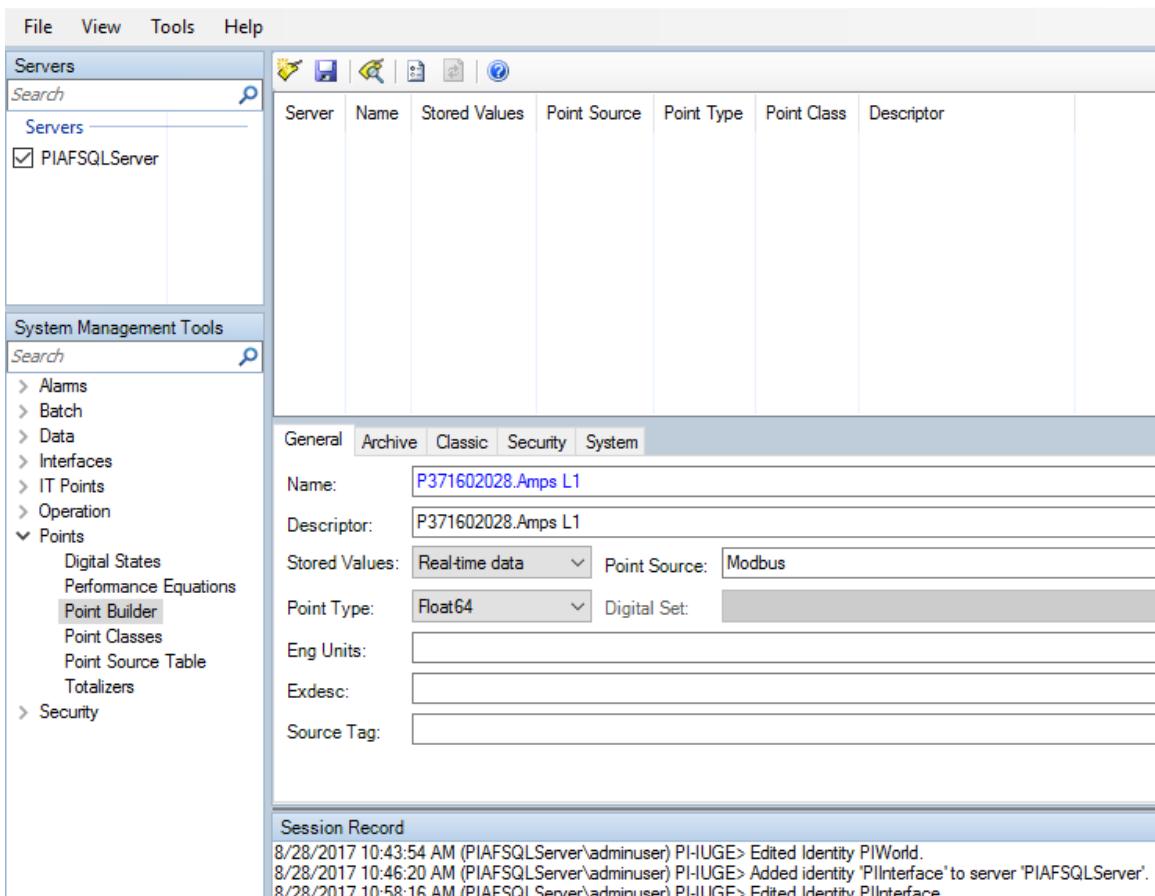
For example1, \\DESKTOP-J9V7ITT**P371602028.Amps L1;UOM=A**
the highlighted part (the text between “\\” and “;”).

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

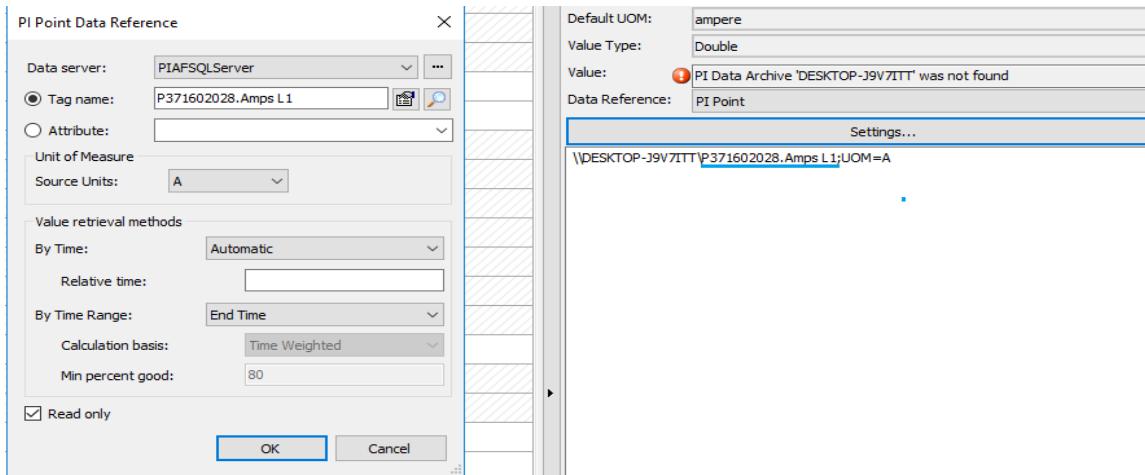
In such cases copy full point after “ \\ ”



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



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



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

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

File View Tools Help

Servers Search

Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor
PIAFSQLServer	P371602028.Amps L1	Real-time data	Modbus	Float64	classic	P371602028.Amps L1
	P371602028.Amps L2	Real-time data	Modbus	Float64	classic	P371602028.Amps L2
	P371602028.Amps L3	Real-time data	Modbus	Float64	classic	P371602028.Amps L3
	P371602028.Amps System Avg	Real-time data	Modbus	Float64	classic	P371602028.Amps System
	P371602028.Daily Electric Cost.60e6094f-e554-5e8f-1742-54def61fbe81	Real-time data	Modbus	Float64	classic	P371602028.Daily Electric
	P371602028.Daily kWh System.3b67c63a-d3c7-5b43-1d5b-4d7994c899bc	Real-time data	Modbus	Float64	classic	P371602028.Daily kWh
	P371602028.kW L1	Real-time data	Modbus	Float64	classic	P371602028.kW L1
	P371602028.kW L2	Real-time data	Modbus	Float64	classic	P371602028.kW L2
	P371602028.kW L3	Real-time data	Modbus	Float64	classic	P371602028.kW L3
	P371602028.kW System	Real-time data	Modbus	Float64	classic	P371602028.kW System
PIAFSQL Server	P371602028.Monthly_Electric_Cost.4b1292a6-694f-517e-0c95-10a9779a4f64	Realtime data	Modbus	Float64	classic	P371602028.Monthly_Electric_Cost

System Management Tools

Search

Servers

Alarms Batch Data IT Points Operation Points Security

Digital States Performance Equations Point Builder Point Classes Point Source Table Totalizers

General Archive Classic Security System

Name: NWS_KFNL_WindDirection

Descriptor: NWS_KFNL_WindDirection

Stored Values: Realtime data Point Source: Modbus

Point Type: String Digital Set:

Eng Units:

Exdesc:

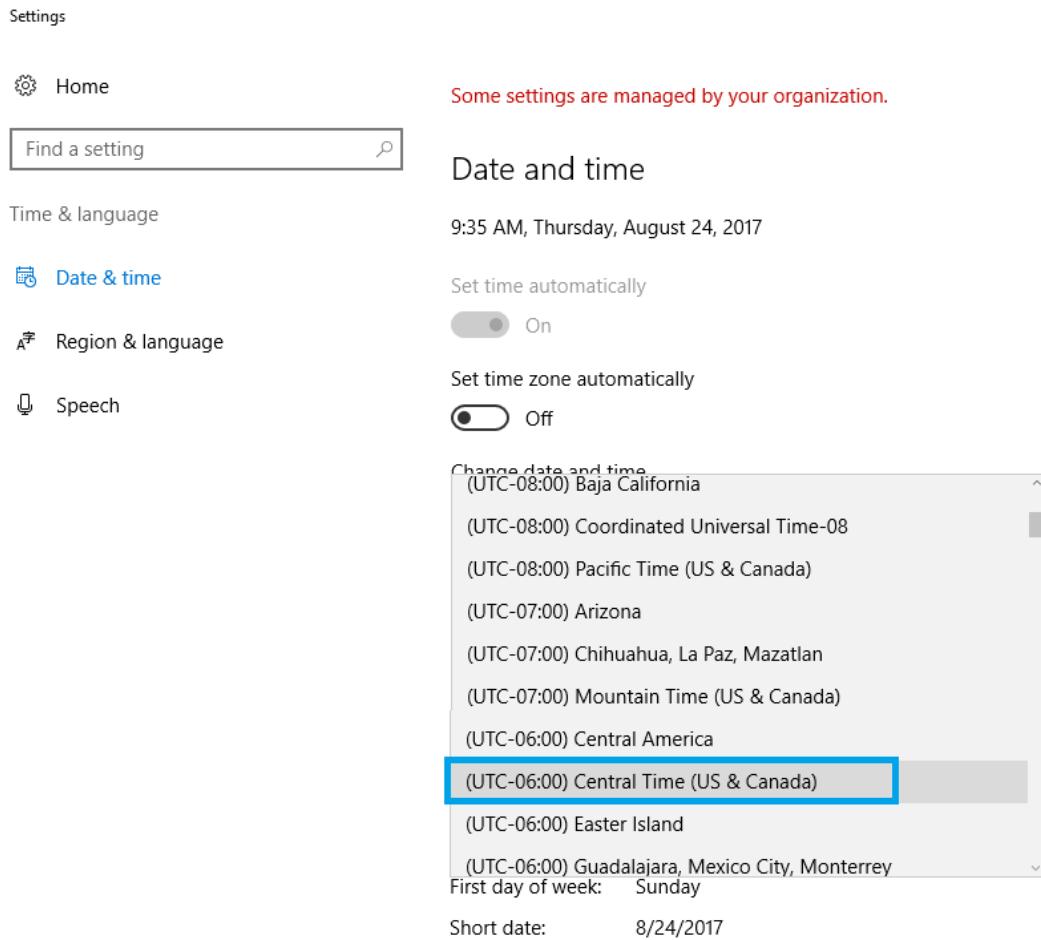
Source Tag:

Session Record

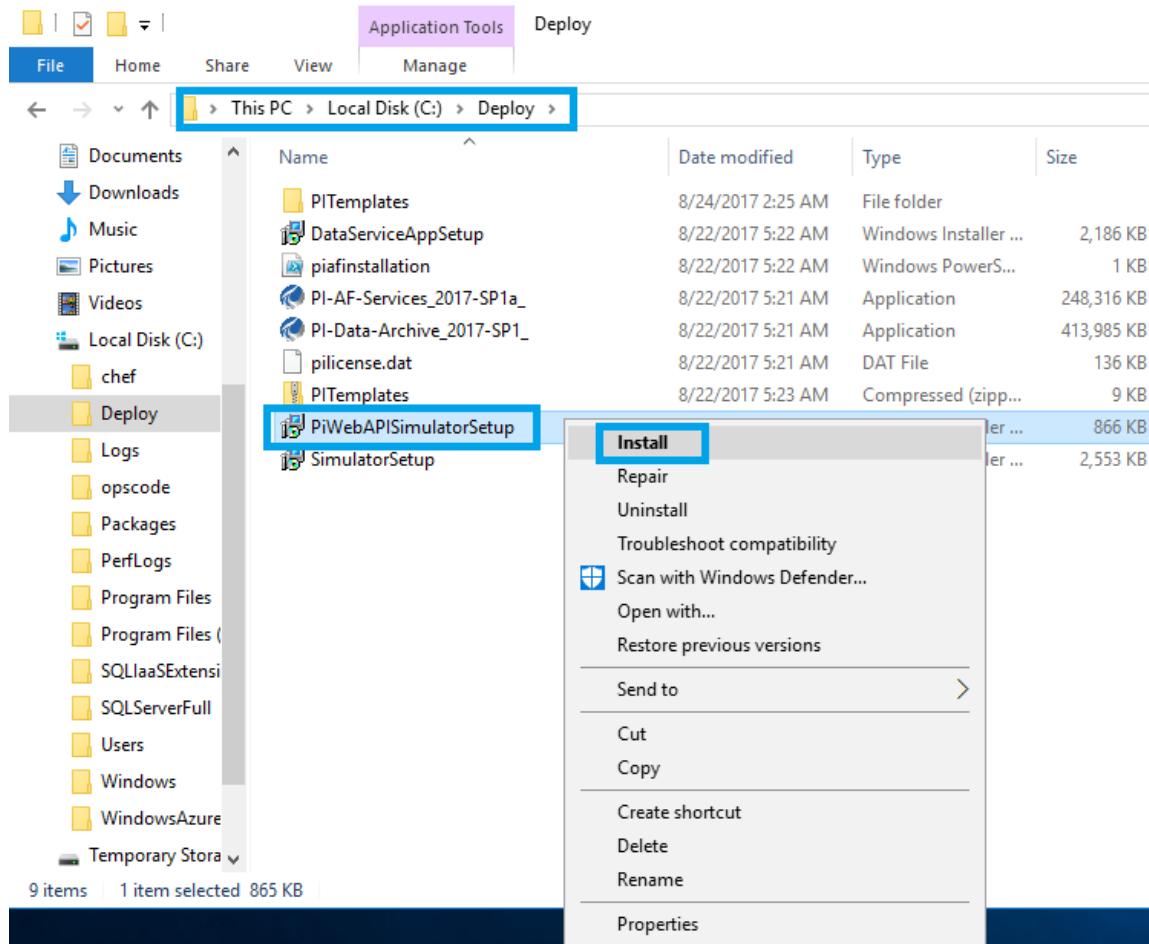
```
8/28/2017 12:32:04 PM (PIAFSQLServer\administrator) PI-PB: Successfully created point P371602030.Volts L2 to Neutral on server PIAFSQLServer.
8/28/2017 12:32:19 PM (PIAFSQLServer\administrator) PI-PB: Successfully created point P371602030.Volts L3 to Neutral on server PIAFSQLServer.
8/28/2017 12:34:22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

9.10. Install And Run The Piweb Simulator Setup

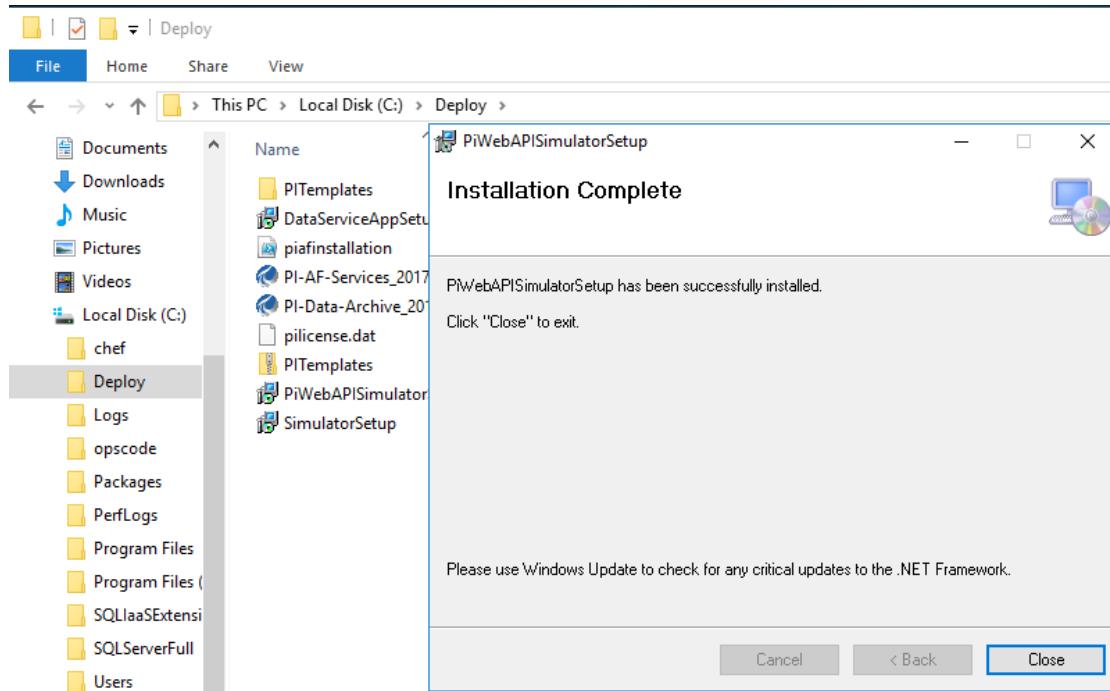
1. Change the time stamp to **(UTC-06:00) Central Time (US&Canada)**



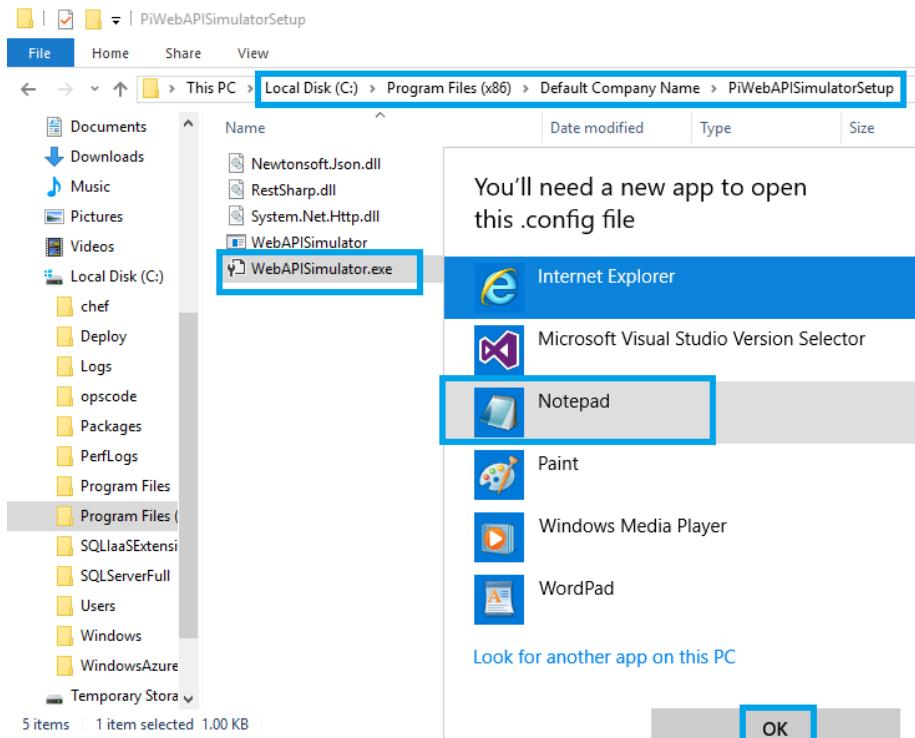
2. Navigate to the **Local Disk (C:) > Deploy > PIWebAPISimulatorSetup** and right-click to **Install**.



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



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



5. Update the Values under Appsettings section as below.

Replace the Username value with your domainnamewithout.com\PIAFSQLServerusername

Replace the Password value with your PIAFSQLServer VM password

Replace the BaseURL with while doing the 9.3.PI web API utility step 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**.

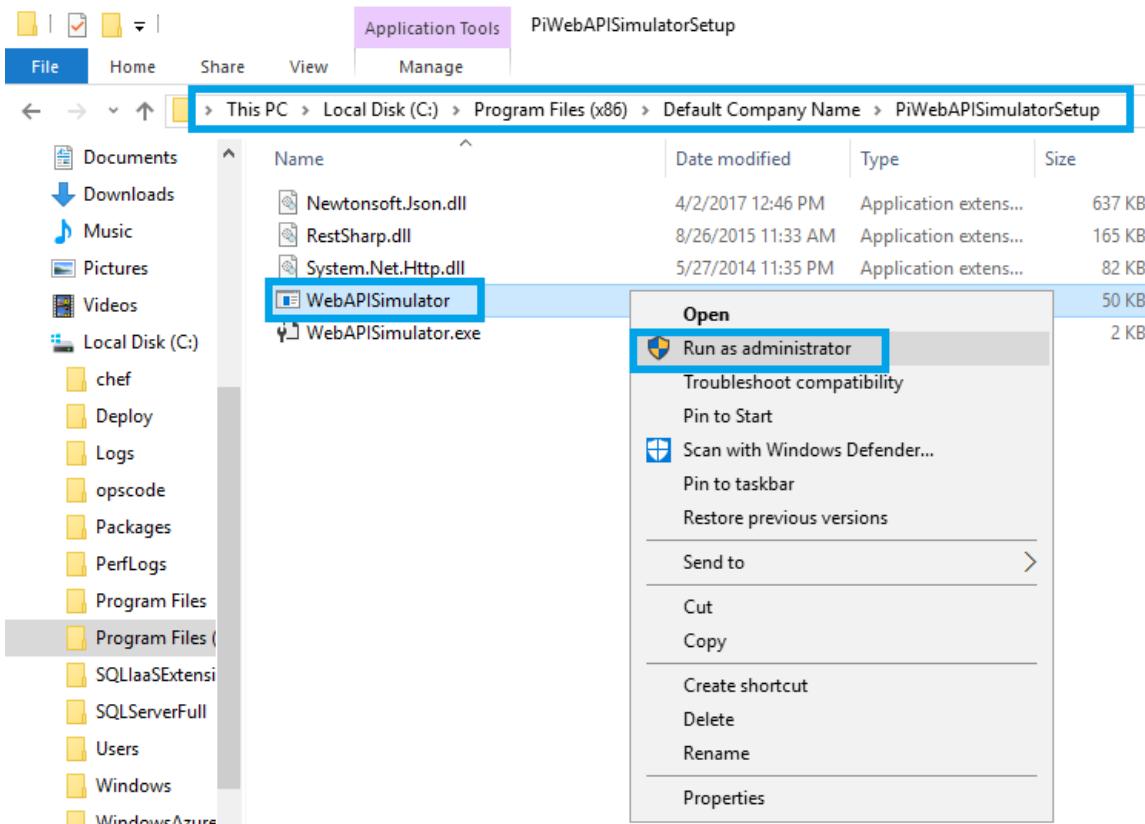
WebAPISimulator.exe - Notepad

```

File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <appSettings>
    <add key="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" />
  </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 c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** no response created *****
Completed Status code is: Accepted
Status Description: Accepted
for powerscout P371602020
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: Accepted
Status Description: Accepted
Done with processing of building :: Building 2
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2FpbmlvdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTlZNA==
***** Response created *****
Completed Status code is: Accepted
Status Description: Accepted
Complete time entry: 9/24/2017 6:13:26 PM
=====Done with timestamparter values, press any key to Exit
```

8. Paste the URL <https://piafsqlserver.sysgainiot.com/piwebapi/> in **Internet Explorer** to view the Data servers URLs.



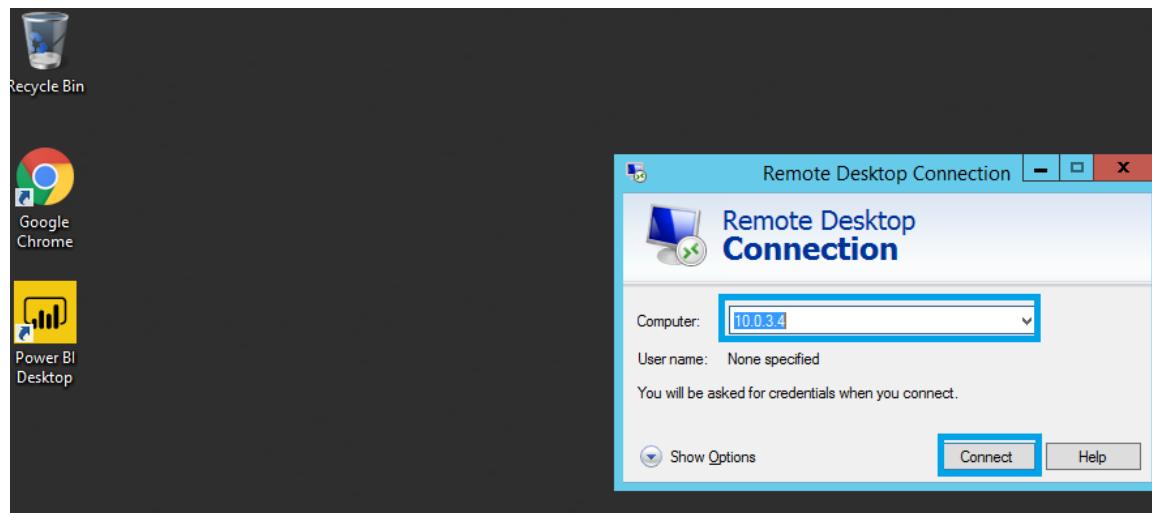
9. To view the **Asset server** links, copy the Asset server link paste it in browser you can the Asset server links, click on databases to view the configuration and energy management items

```

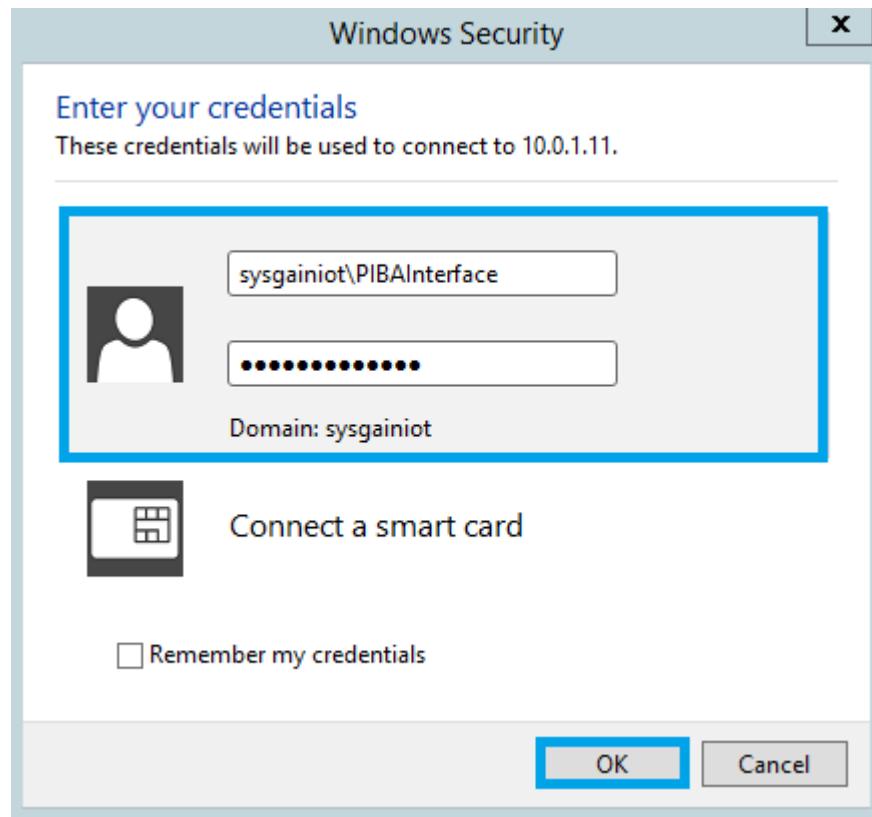
{
  "Links": {},
  "Items": [
    {
      "WebId": "DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90",
      "Id": "deea162d-9eac-4945-82e1-4a1e9baa8d8e",
      "Name": "Configuration",
      "Description": "A store for configuration data.",
      "Path": "\\\PIAFSQLServer\\Configuration",
      "ExtendedProperties": {}
    },
    {
      "Links": {
        "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90",
        "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/e/elements"
      }
    },
    {
      "ElementTemplate": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/elementTemplate"
    },
    {
      "EventFrames": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/eventFrames"
    },
    {
      "AssetServer": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/SO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/assetServer"
    },
    {
      "ElementCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/elementCategories"
    },
    {
      "AttributeCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/attributeCategories"
    },
    {
      "TableCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/tableCategories"
    },
    {
      "AnalysisCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/analysisCategories"
    },
    {
      "EnumerationSets": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/enumerationSets"
    },
    {
      "Tables": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/tables"
    },
    {
      "Security": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/security"
    },
    {
      "SecurityEntries": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/securityEntries"
    }
  ],
  "Links": {
    "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90",
    "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gLabh3qyeRUmC4Uoem6qdjgUE1BR1NRTNFU1ZFU1xDT05GSUdVUkFUS90/e/elements"
  }
},
{
  "WebId": "DO1zeX08j8WUKd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U",
  "Id": "18927245-d4f3-46ab-8f4bcb250e",
  "Name": "EnergyManagement",
  "Description": "",
  "Path": "\\\PIAFSQLServer\\EnergyManagement",
  "ExtendedProperties": {}
},
{
  "Links": {
    "Self": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U",
    "Elements": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U/e/elements"
  }
},
{
  "ElementTemplate": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U/elementTemplate"
},
{
  "EventFrames": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gRXKSGPPUq0a2q49EvL41DgUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U/eventFrames"
},
{
  "AssetServer": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/SO1zeX08j8WUKd8kLeW7hI7gUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U/assetServer"
},
{
  "ElementCategories": "https://piafsqlserver.sysgainiot.com/piwebapi/assetdatabases/DO1zeX08j8WUKd8kLeW7hI7gUE1BR1NRTNFU1ZFU1xFTkVSR11NQUSBROVRNU5U/elementCategories"
}
  
```

10. Installation of PI BA Integrator

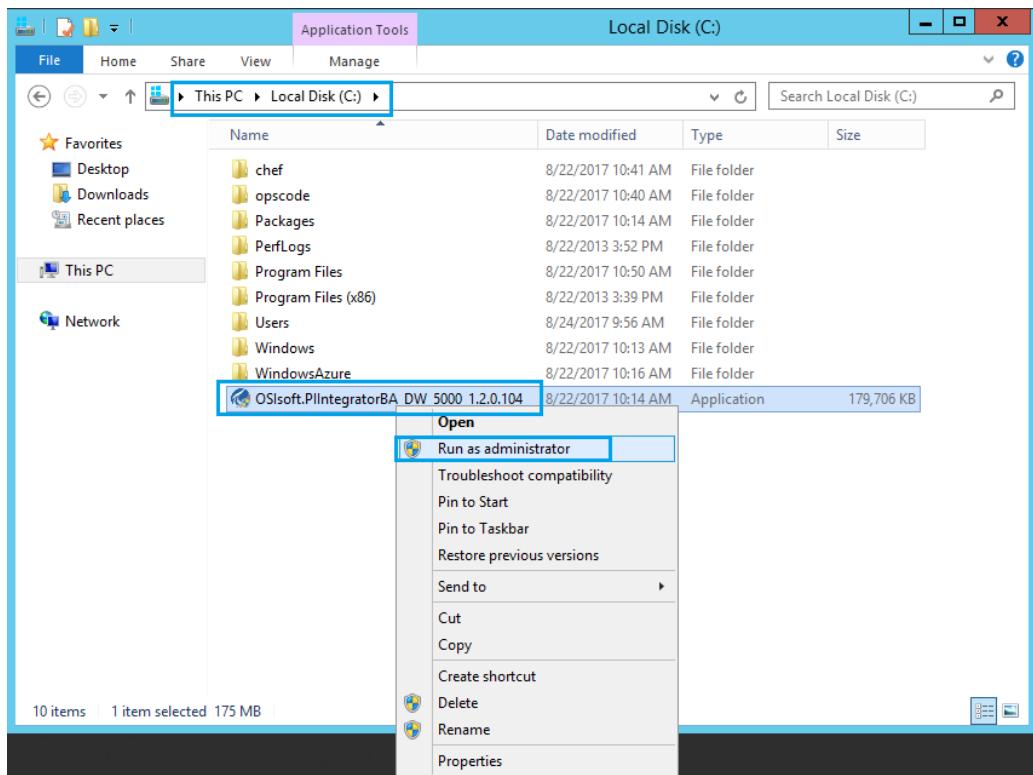
- From Bastion server, connect to the Remote server PIBA VMserver with details provided in output section.



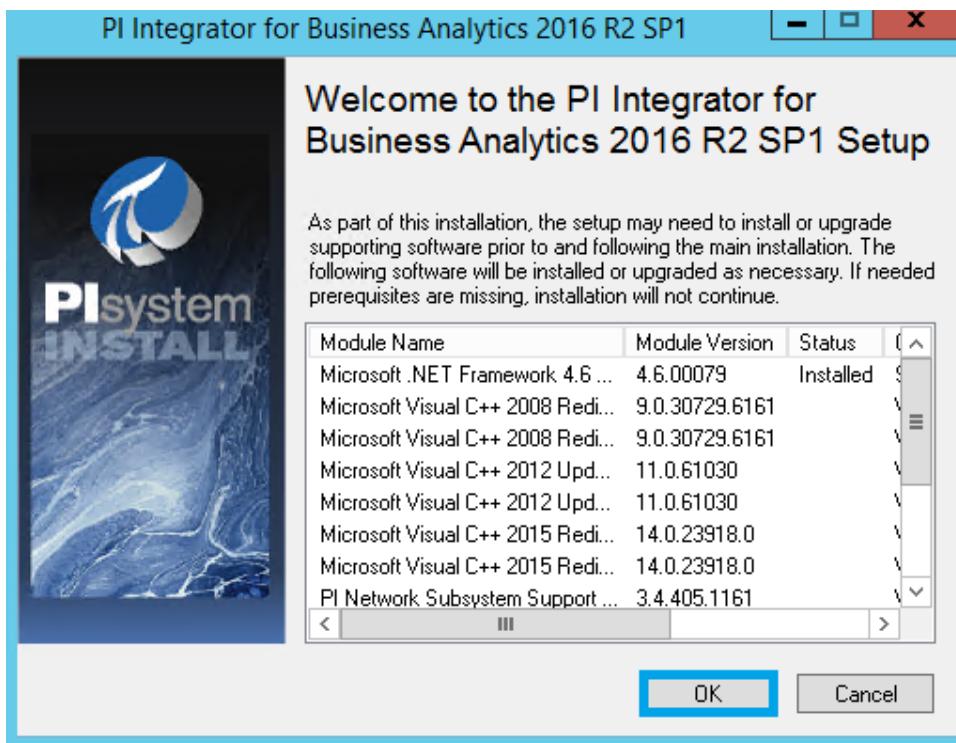
2. Login with credentials "<domainname>\PIBAInterface" (user you created in AD server) and **password**.



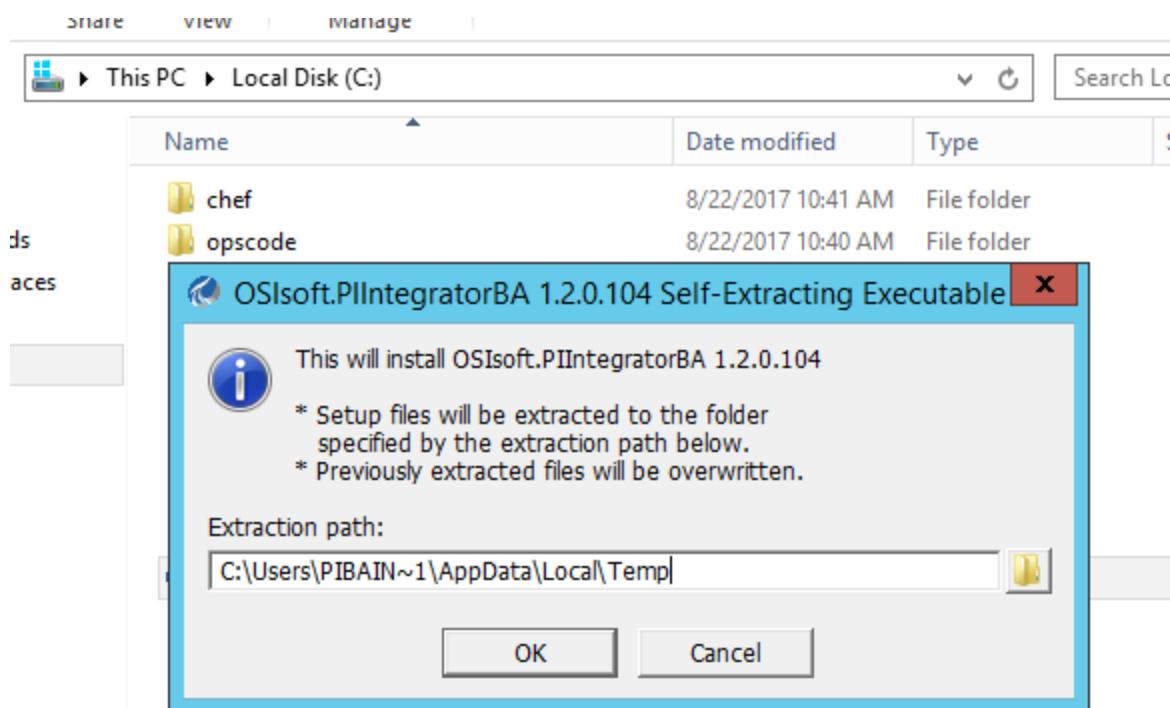
3. After connecting to the PIBA VMServer, navigate to the LocalDisk (C:) and select **OSISoft.PIIntegratorBA**, then right-click on and **Run as administrator**.



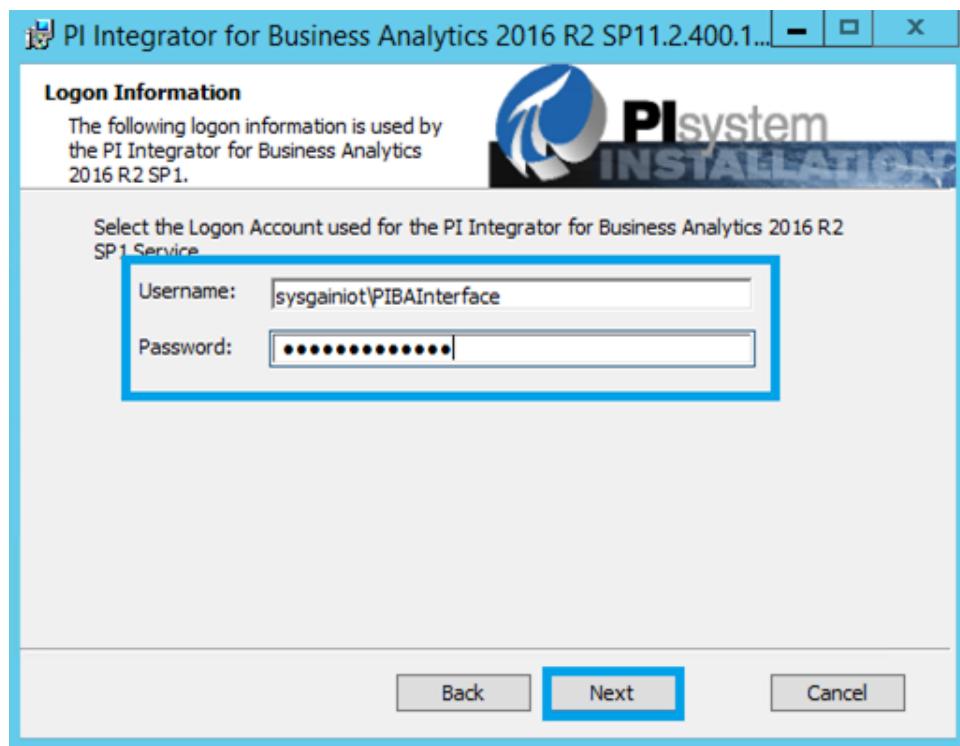
4. Click on **Ok**.



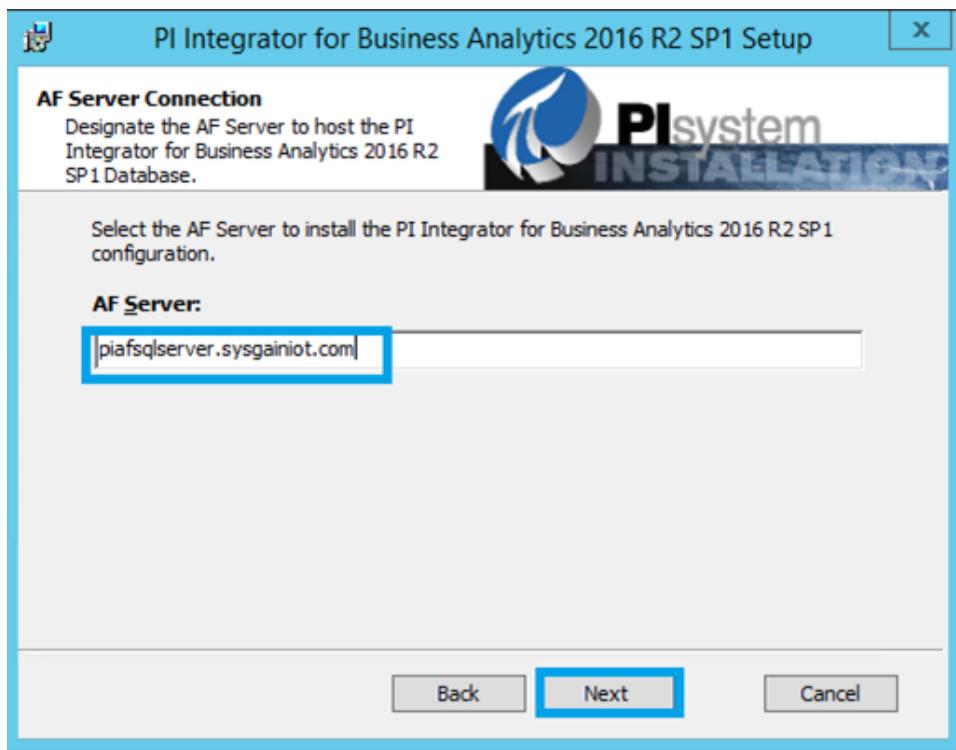
5. Click on **OK**



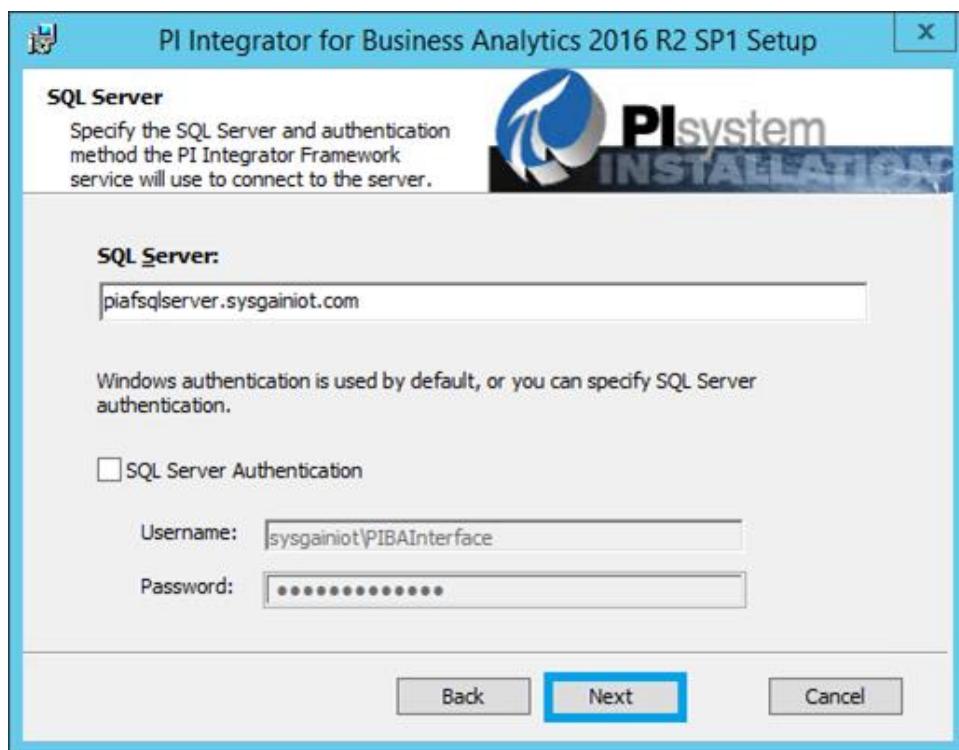
6. Give the same credentials which you used to login to PIBA server in Logon credentials and click on **Next**



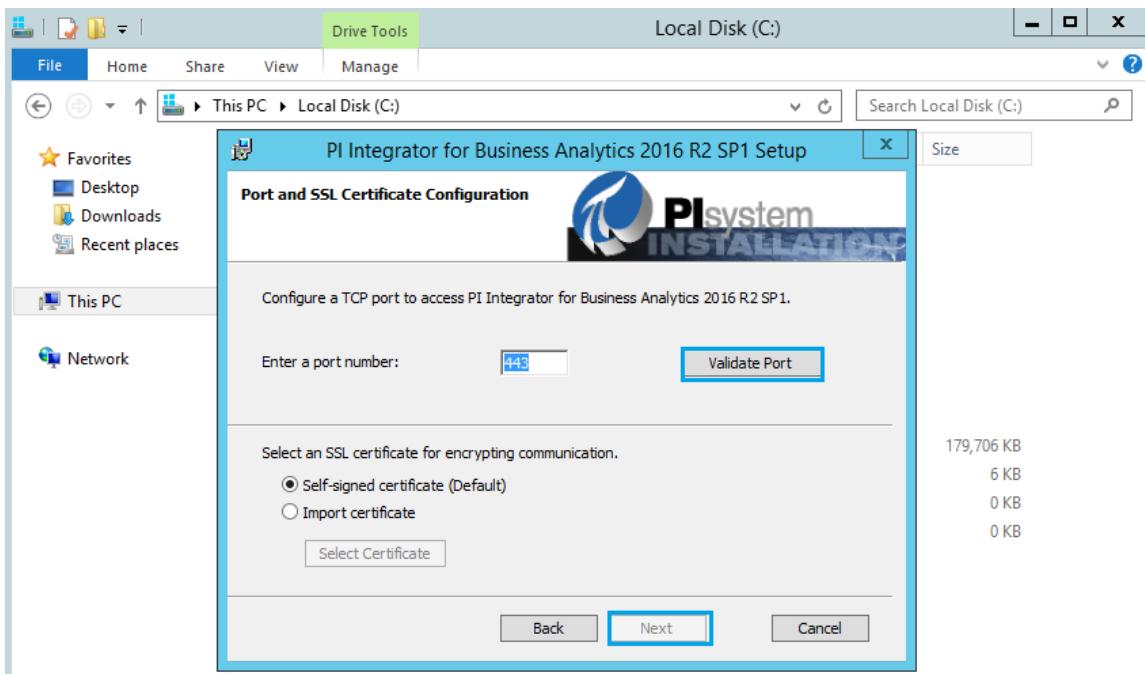
7. Give the Af sever link as piafsqlserver.<domainname> to host PIBA database and click on **Next**



Click on **Next**

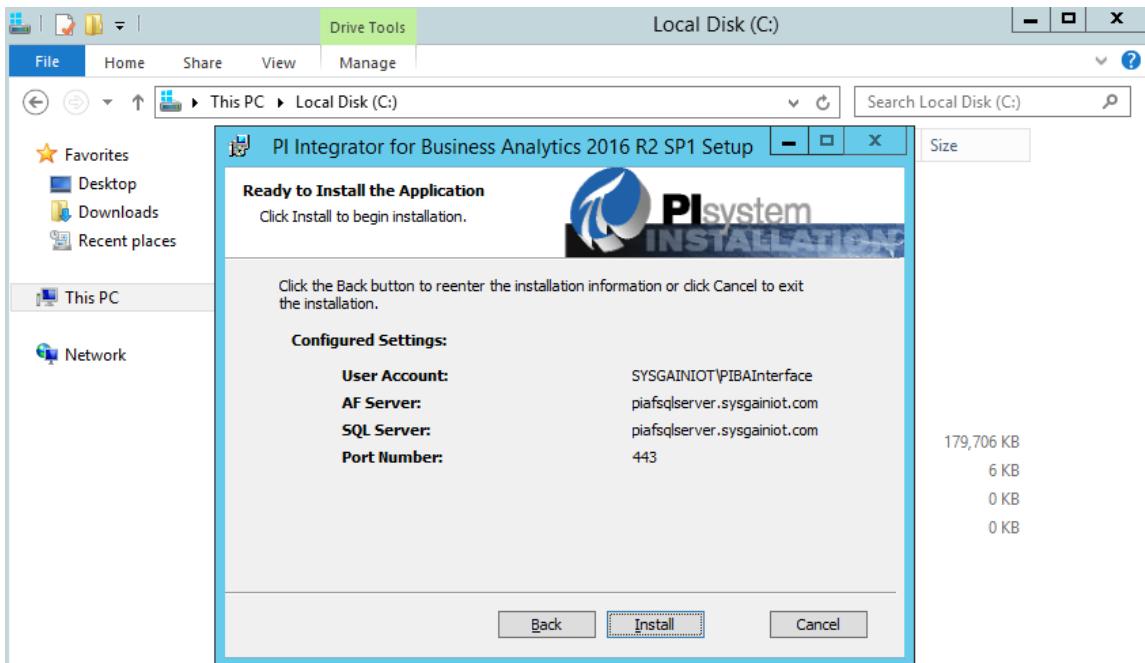


8. Click on **Validate port**, then **Next**.



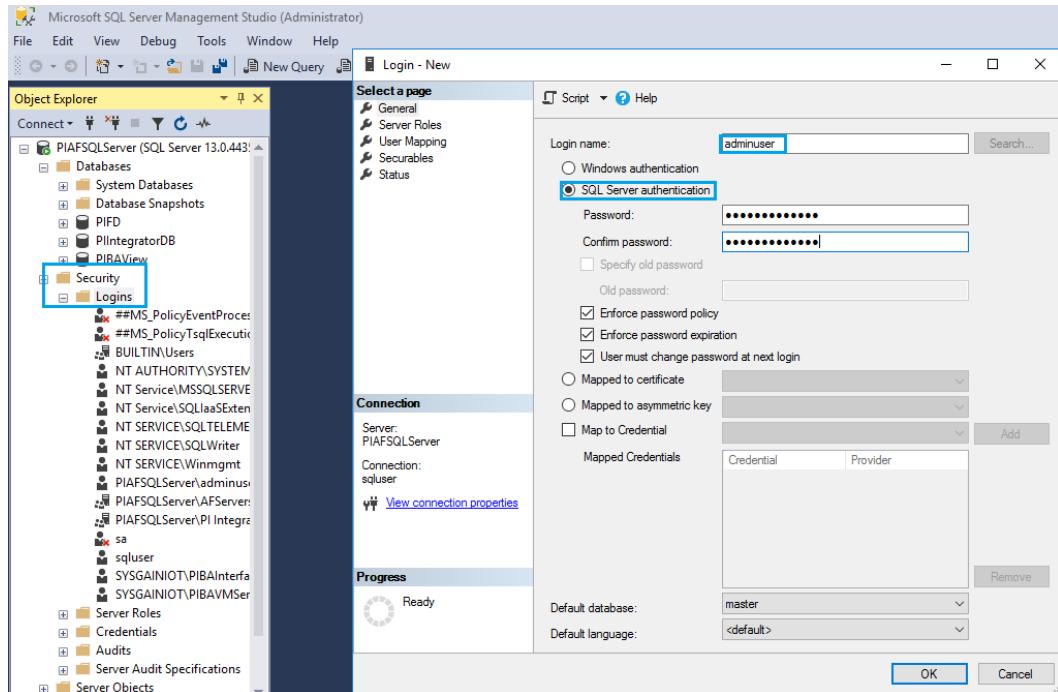
10.

Click on **Install**.

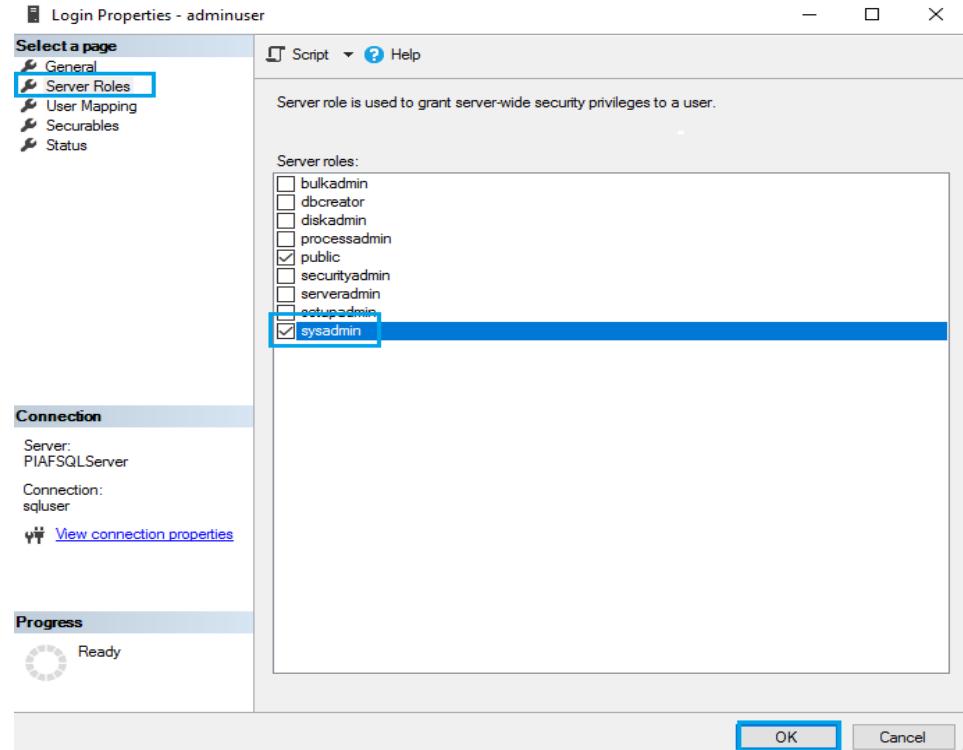


10.1. Configuring PI Business Analytics

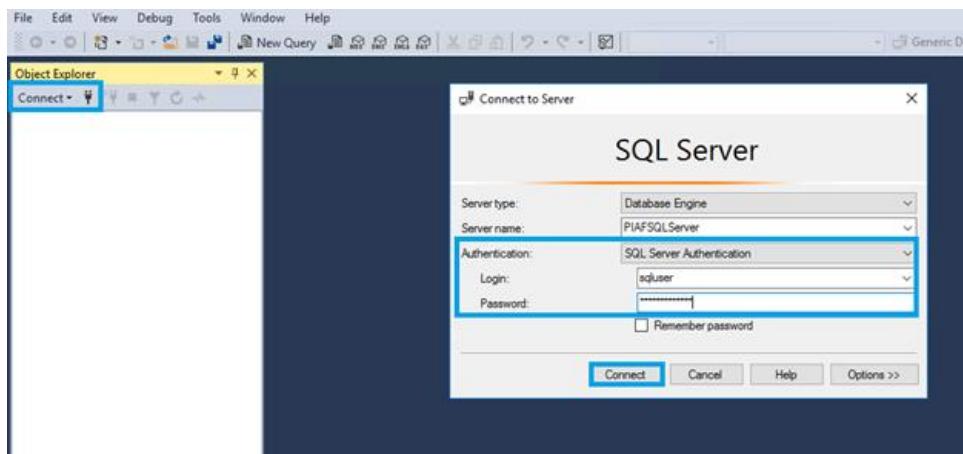
1. In Bastion Server, connect to the PIAFSQLServer with the credentials provided in the output section.
2. Go to the **Security** section, then right-click on **Login** and select **New Login**. Set the login name as **adminuser** and select **SQL Server Authentication**. Set a password, then click on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



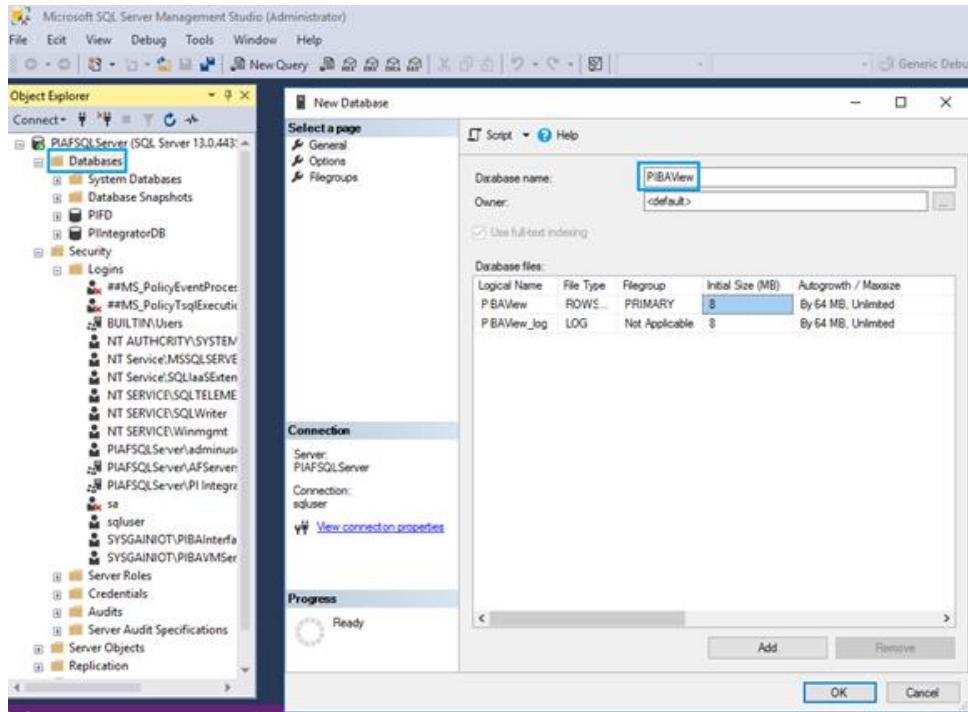
3. Right-click on the admin user under **Login** and select **Properties**. On the Properties screen, select **Server Roles**, then check **sysadmin** and click **Ok**.



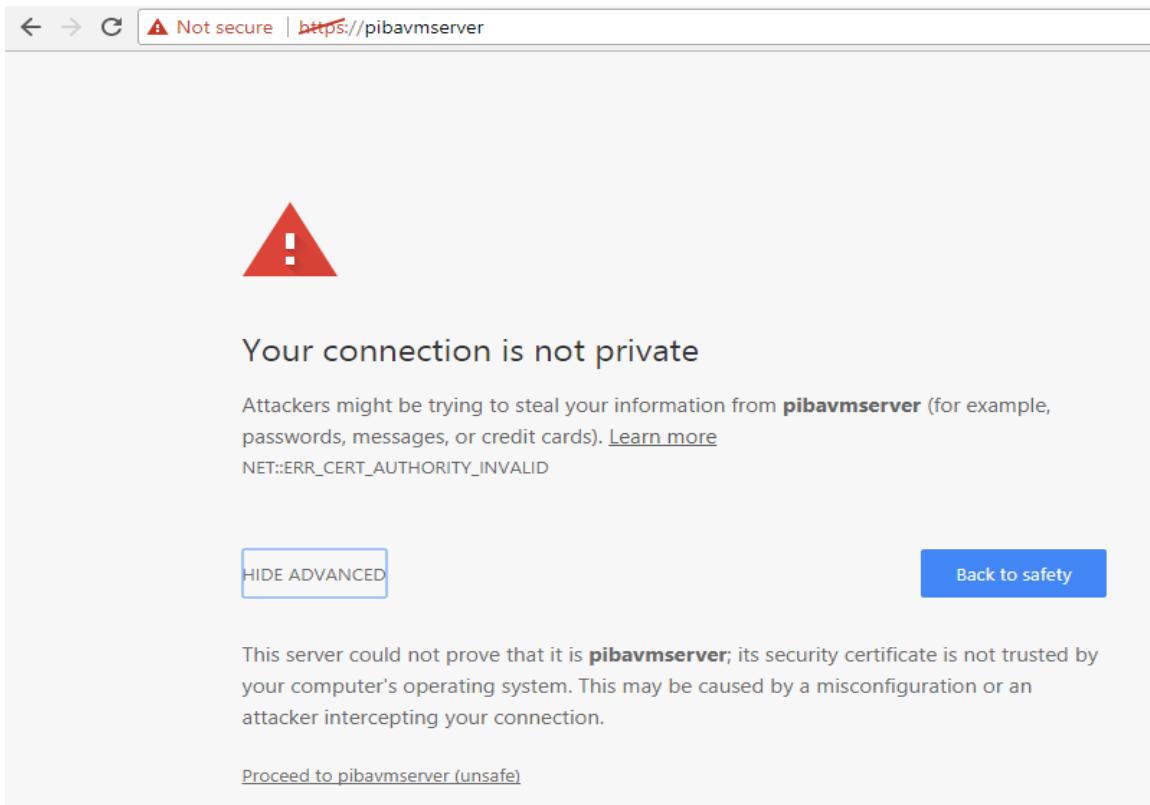
4. Disconnect and Click on connect in **ssms** to login with SQL Servr authentication to create database with following SQL credentials



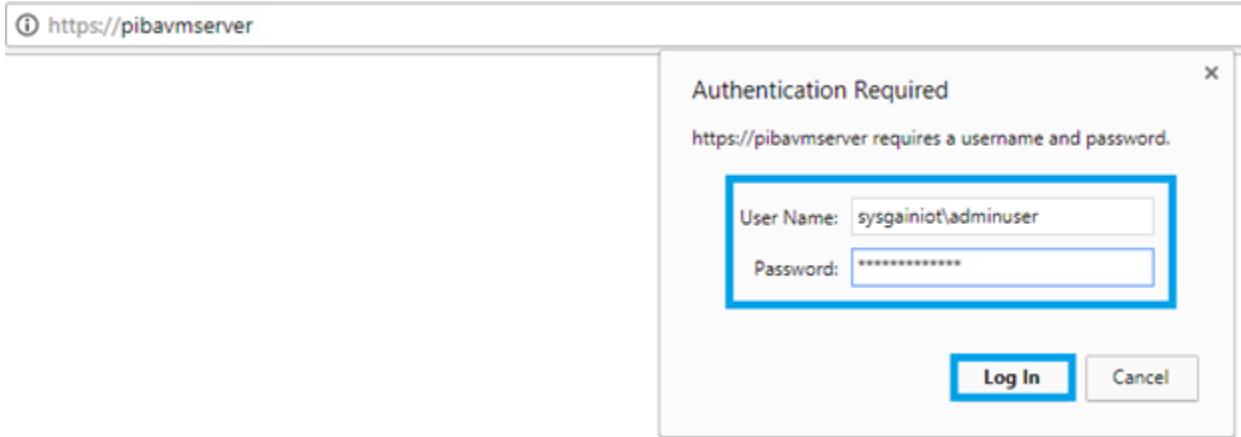
5. Go to the **SQLServer Management Studio**, right-click on **Database**, select **New Database**, and give the Database name as **PIBAView**. Click on **Ok**.



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



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



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

The screenshot shows the PI Integrator for Business Analytics interface. The top navigation bar includes icons for back, forward, search, and a red 'Not secure' warning for the URL <https://pibavmserver>. Below the bar are four buttons: 'Create Asset View', 'Create Event View', 'Modify View', and 'Remove View'. A table below lists columns for Lock, Name, Run Status, and Type. The table body is currently empty.

3. Click on **Administration**.

The screenshot shows the PI Integrator for Business Analytics web interface. The URL in the address bar is <https://pibavmserver>, with a red warning icon indicating it's not secure. The main menu on the left includes "My Views", "Create New Asset View", "Create New Event View", and "Administration". The "Administration" section is highlighted with a blue box. The right side of the screen shows a "View" dialog box with options like "View", "Modify View", and "Remove". Below the dialog is a "Run Status" table.

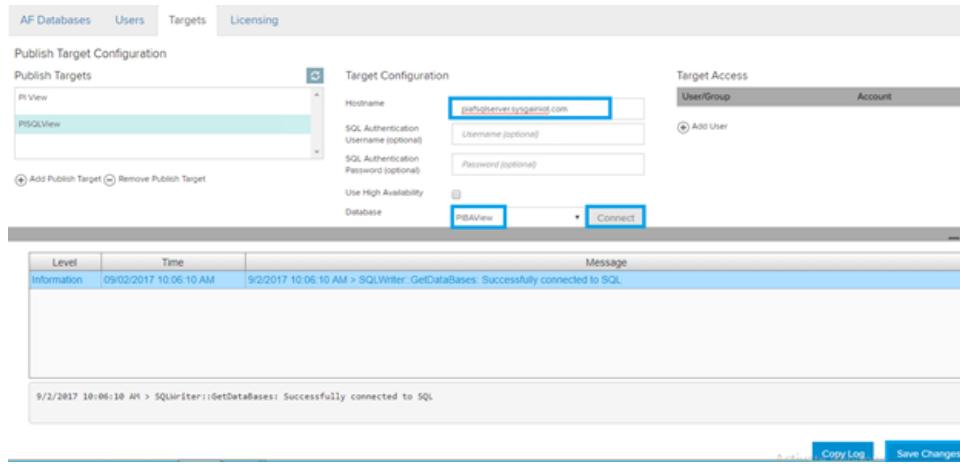
4. Select Targets > Add Publish Target.

Enter Target Name as **PISQLView**.

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

The screenshot shows the "Administration" section of the PI Integrator web interface, specifically the "Targets" tab. A modal window titled "Create a New Publish Target" is open. It contains fields for "Target Name" (set to "PISQLView") and "Target Type" (set to "Microsoft SQL Server"). At the bottom of the modal are "Cancel" and "Create New Target" buttons. The background shows a list of existing targets, with one entry labeled "PI View".

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**

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**.

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

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

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

The screenshot shows the 'Select Data > Modify View' interface. On the left, there's a tree view of 'Source Assets' under 'PIAFSQLServer' and 'EnergyManagement'. Under 'Assets', 'Building 1' is expanded, showing 'P371602028' and 'P371602030', with 'P371602028' selected. The 'Attributes' section lists various power parameters like Amps L1, L2, L3, and System Avg. On the right, a 'Search Shape' panel is open, showing a list of matches with a blue border around the top item: 'P371602018'. A message box says 'Found 4 Matches'.

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

The screenshot shows the 'Edit Value Mode' view. At the top, there are buttons for 'Add Column', 'Edit Row Filters', and 'Edit Value Mode' (which is highlighted with a blue border). Below that is a table with columns: PowerScout,TimeStamp, Amps L1, Amps L2, Amps L3, Amps System Avg, and Breaker Data. The table contains numerous rows of data, all corresponding to 'P371602028' and timestamped at 8/24/2017 3:31:27.473 AM. The 'Breaker Data' column shows repeated entries of 'New (2018) 4th floor p:'. There are also 'Start Time' and 'End Time' fields with a 'Back' button and a 'Next' button.

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

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

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

The screenshot shows the 'Target Configuration' dropdown set to 'PISQLView'. Below it, two radio buttons are shown: 'Run Once' (unchecked) and 'Run on a Schedule' (checked). Under 'First Run', there is a field containing an asterisk (*). Below that, 'Recur every' is set to '5 minutes'. To the right, a 'Summary' box contains the following text:

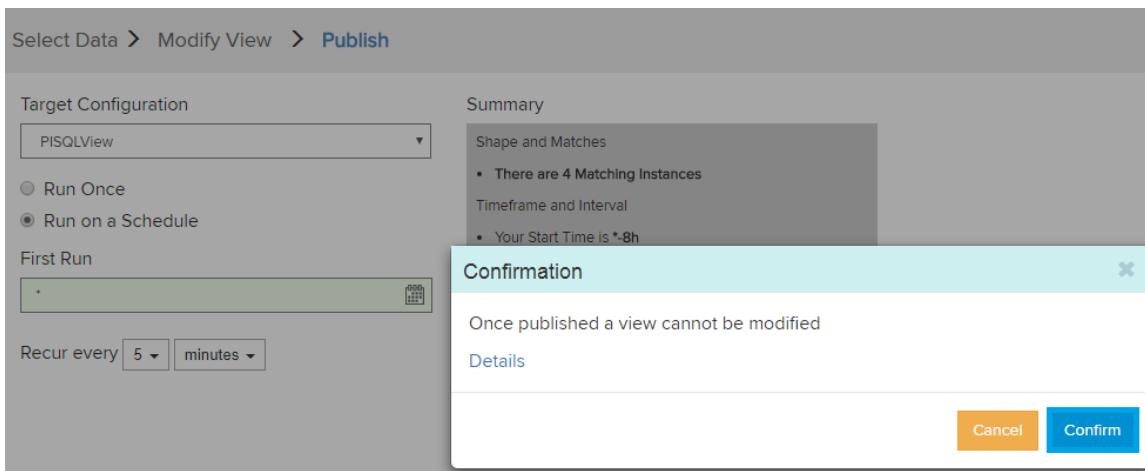
- There are 4 Matching Instances

Timeframe and Interval

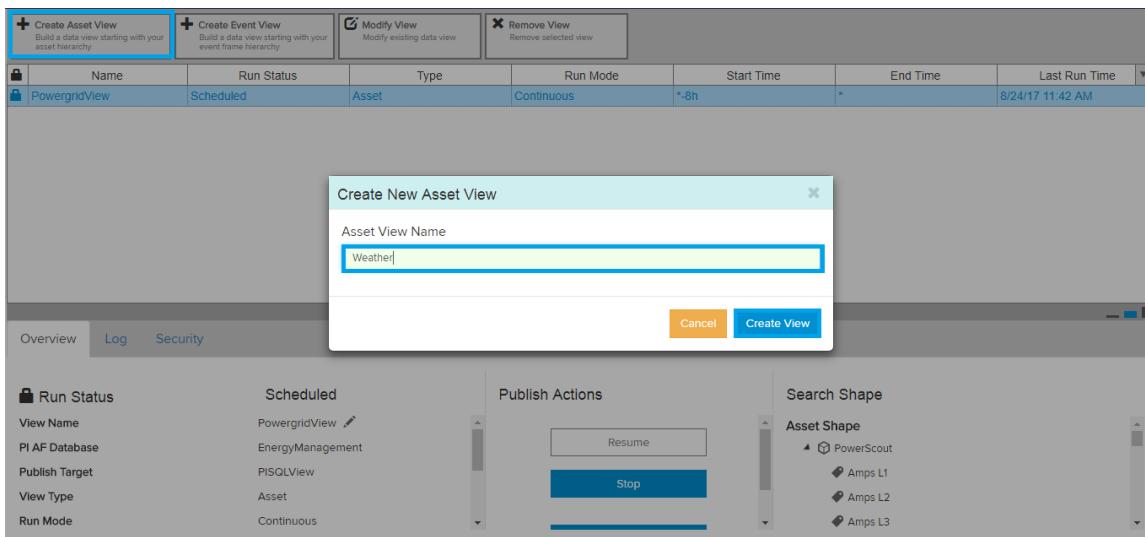
- Your Start Time is *-8h
- Your End Time is *
- Your Time Interval gets an interpolated measurement based on column Amps L1

A large blue 'Publish' button is located at the bottom right of the configuration area.

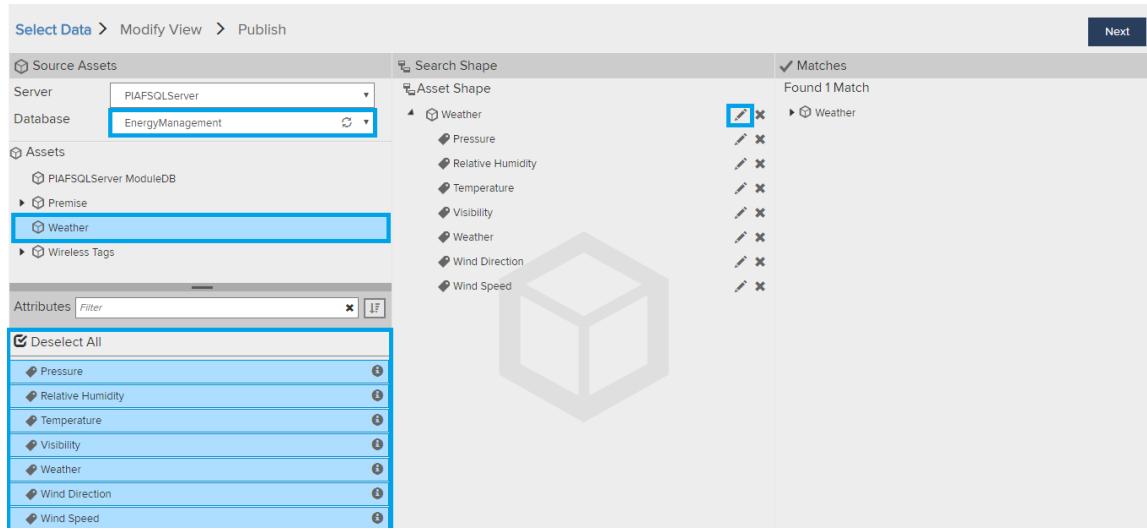
14. Click on Confirm.



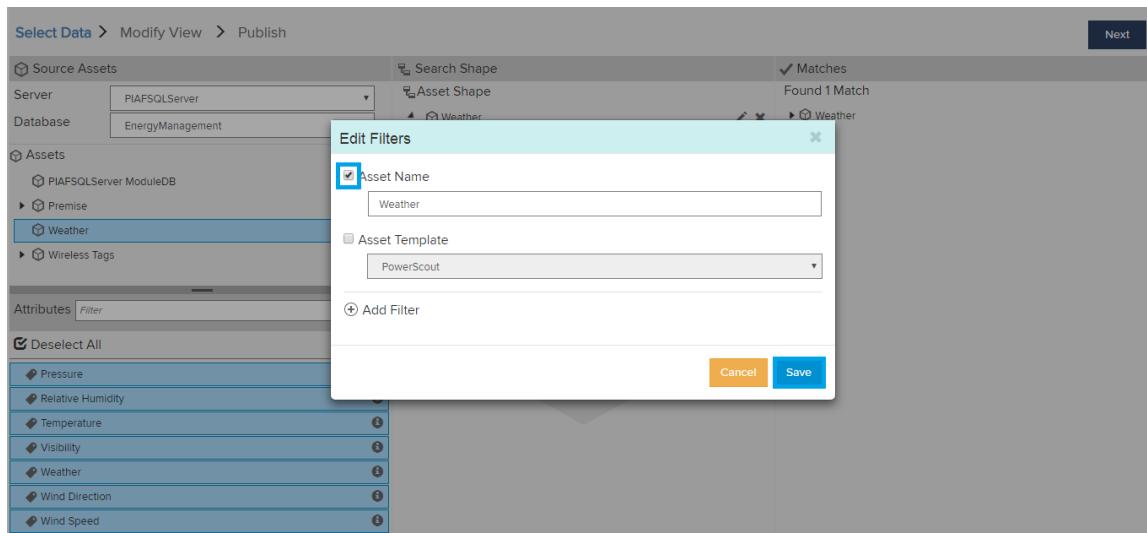
15. Create another Asset view by clicking on **Create asset view, name it **Weather**, then click on **Create view**.**



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



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



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

Select Data > Modify View > Publish

Source Assets

Server: PIAFSQLServer
Database: EnergyManagement

Assets

- 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
- Weather
- Wind Direction
- Wind Speed



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

Select Data > Modify View > Publish									
+ Add Column 9 columns		Edit Row Filters 0 Row Filters		Edit Value Mode Interpolated Values Key on Pressure		Start Time -1h		End Time	
Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Wind Direction	Wind Speed	
Weather	8/24/2017 4:48:07.4...	29.207	30.171	51.801	3.017	Overcast	North	7.241	
Weather	8/24/2017 4:49:07.3...	31.213					Variable	19.281	
Weather	8/24/2017 4:49:42.2...	31.922					Northwest	23.531	
Weather	8/24/2017 4:50:07.1...	29.220					North	7.320	
Weather	8/24/2017 4:50:42.1...	30.709					Southeast	16.255	
Weather	8/24/2017 4:51:06.9...	29.011					Mist		
Weather	8/24/2017 4:51:41.9...	30.932					North	6.064	
Weather	8/24/2017 4:52:06.8...	28.928					Southeast	17.590	
Weather	8/24/2017 4:52:41.8...	29.719					West	5.566	
Weather	8/24/2017 4:53:06.7...	31.715					Cloudy	10.314	
Weather	8/24/2017 4:53:41.7...	28.506					South		
Weather	8/24/2017 4:54:06.5...	31.938	30.490	22.973	3.044	Thunderstorms	Northwest	22.290	
Weather	8/24/2017 4:54:41.6...	30.639	65.982	72.929	6.598	Light Rain	Southeast	23.625	
Weather	8/24/2017 4:55:06.4...	28.160	4.002	36.361	0.400	Fog/Mist	North	15.836	
Weather	8/24/2017 4:55:41.5...	30.862	71.546	76.212	7.155	Light Rain	East	0.960	
Weather	8/24/2017 4:56:06.3...	30.947	73.686	77.474	7.369	A Few Clouds	Southeast	17.171	
Weather	8/24/2017 4:56:41.3...	28.214	5.349	37.156	0.535	A Few Clouds	South	17.685	
Weather	8/24/2017 4:57:06.2...	29.735	43.369	59.588	4.337	unknown Precip	East	1.284	
Weather	8/24/2017 4:57:41.2...	28.437	10.913	40.439	1.091	Fair and Breezy	South	10.409	

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

Select Data > Modify View > Publish									Back	Next
Add Column 9 columns		Edit Row Filters 0 Row Filters		Edit Value Mode Interpolated Values Key on Pressure		Start Time	End Time	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	17.685		
Weather	8/24/2017 4:56:41.3...	28.214	5.349	37.156	0.535	unknown Precip	East	1.284		
Weather	8/24/2017 4:57:06.2...	29.735	43.369	59.588	4.337	Fair and Breezy	South	10.409		
Weather	8/24/2017 4:57:41.2...	28.437	10.913	40.439	1.091	A Few Clouds	East	2.619		

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

Select Data > Modify View > Publish

Target Configuration

PISQLView

Run Once

Run on a Schedule

First Run

*

Recur every **5** minutes

Summary

Shape and Matches

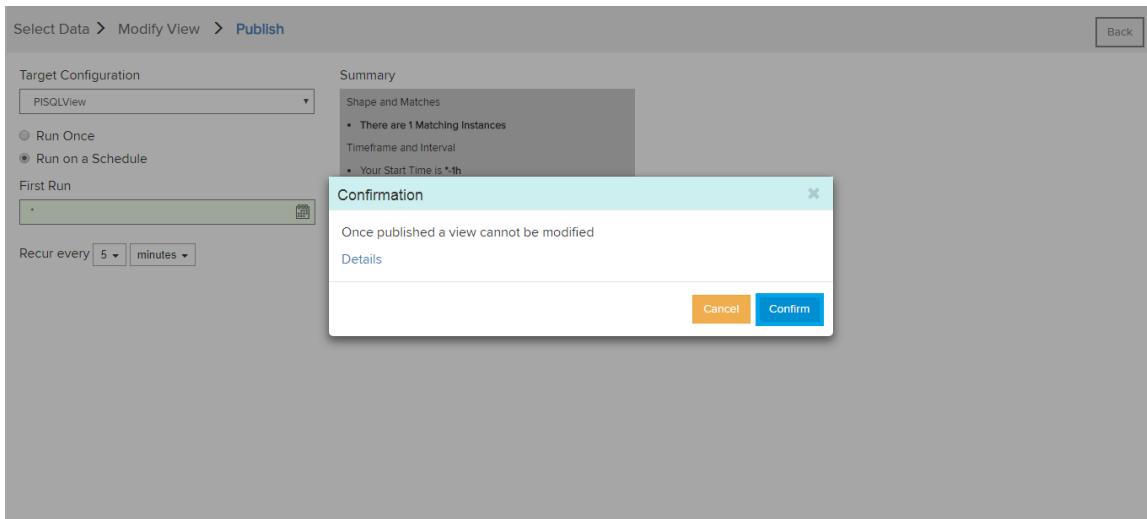
- There are 1 Matching Instances

Timeframe and Interval

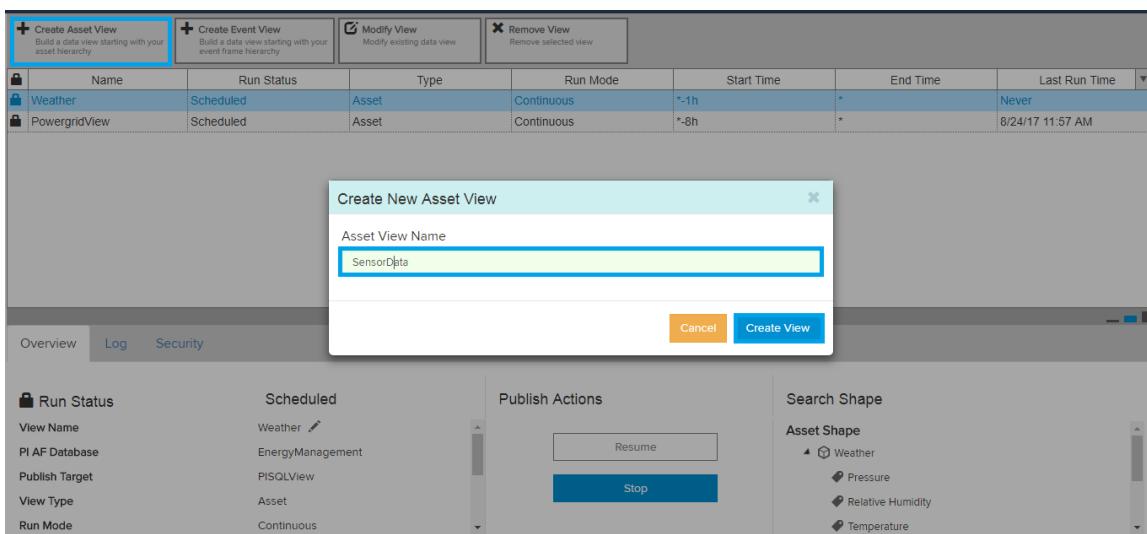
- Your Start Time is ***-1h**
- Your End Time is *****
- Your Time Interval gets an interpolated measurement based on column **Pressure**

Publish

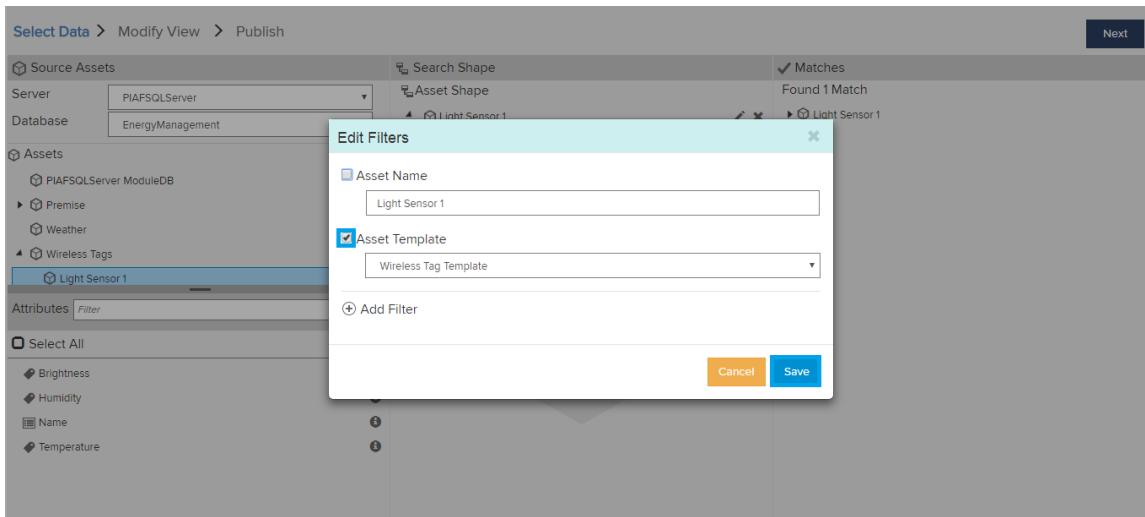
22. Click on Confirm.



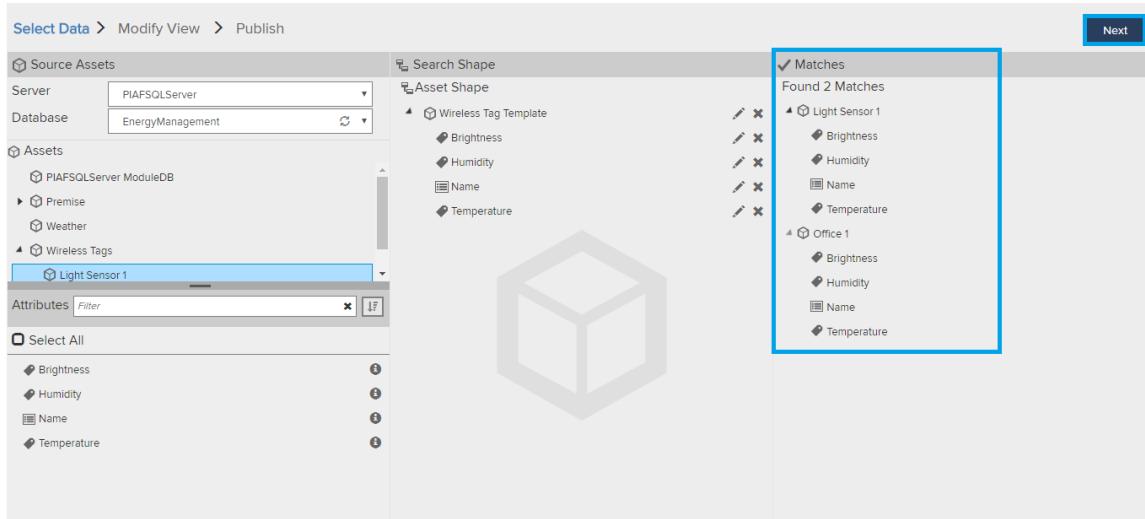
23. Create another Asset view with the name **SensorData and click on **Create View**.**



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



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



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

Select Data > Modify View > Publish

Start Time: ~8h End Time: * Apply

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			1	
Light Sensor 1	8/24/2017 4:05:18.956 AM			1	
Light Sensor 1	8/24/2017 4:06:18.956 AM			1	
Light Sensor 1	8/24/2017 4:07:18.956 AM			1	
Light Sensor 1	8/24/2017 4:08:18.956 AM			1	
Light Sensor 1	8/24/2017 4:09:18.956 AM			1	
Light Sensor 1	8/24/2017 4:10:18.956 AM			1	
Light Sensor 1	8/24/2017 4:11:18.956 AM			1	
Light Sensor 1	8/24/2017 4:12:18.956 AM			1	
Light Sensor 1	8/24/2017 4:13:18.956 AM			1	
Light Sensor 1	8/24/2017 4:14:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:15:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:16:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:17:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:18:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:19:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:20:18.956 AM			Light Sensor 1	
Light Sensor 1	8/24/2017 4:21:18.956 AM			Light Sensor 1	

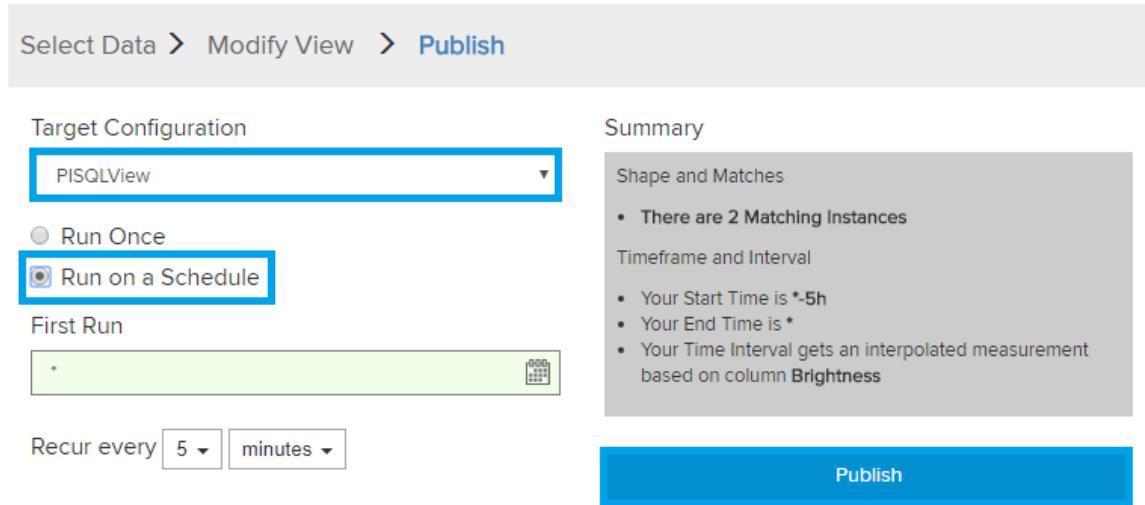
27. Select the start time as ***-5h**, then click **Apply** and click **Next**.

Select Data > Modify View > Publish

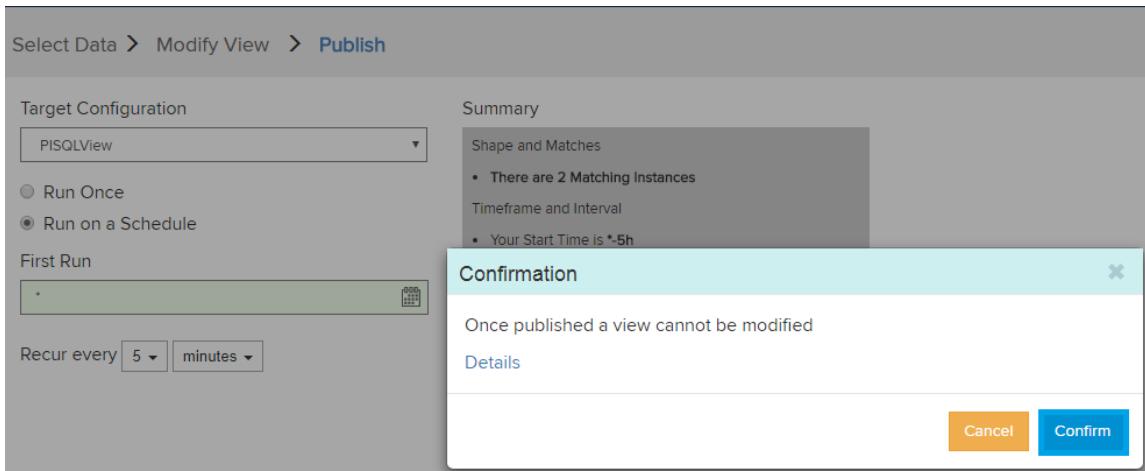
Start Time: *-5h End Time: * Apply

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 4:50:42.080 AM	923.606	36.281	Office 1	55.281
Office 1	8/24/2017 4:51:06.967 AM	2,592.229	51.241	Office 1	70.241
Office 1	8/24/2017 4:51:41.971 AM	1,084.964	37.727	Office 1	56.727
Office 1	8/24/2017 4:52:06.819 AM	1,147.017	38.284	Office 1	57.284
Office 1	8/24/2017 4:52:41.858 AM	205.788	29.845	Office 1	48.845
Office 1	8/24/2017 4:53:06.694 AM	267.841	30.401	Office 1	49.401
Office 1	8/24/2017 4:53:41.736 AM	2,226.611	47.963	Office 1	66.963
Office 1	8/24/2017 4:54:06.580 AM	1,814.165	44.265	Office 1	63.265
Office 1	8/24/2017 4:54:41.618 AM	2,387.969	49.409	Office 1	68.409
Office 1	8/24/2017 4:55:06.464 AM	1,975.524	45.712	Office 1	64.712
Office 1	8/24/2017 4:55:41.496 AM	1,508.793	41.527	Office 1	60.527

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



29. Click on **Confirm**.



30. After creating the Asset Views, check in **PISQLAFServer** in **SQL Server Management Studio**, 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 SQL Server Management Studio interface. The Object Explorer on the left shows the database structure, including the PIBAView database and its tables. The central pane displays a query results grid for the 'Weather' table, showing 744 rows of data. The Properties pane on the right provides connection details for the current session.

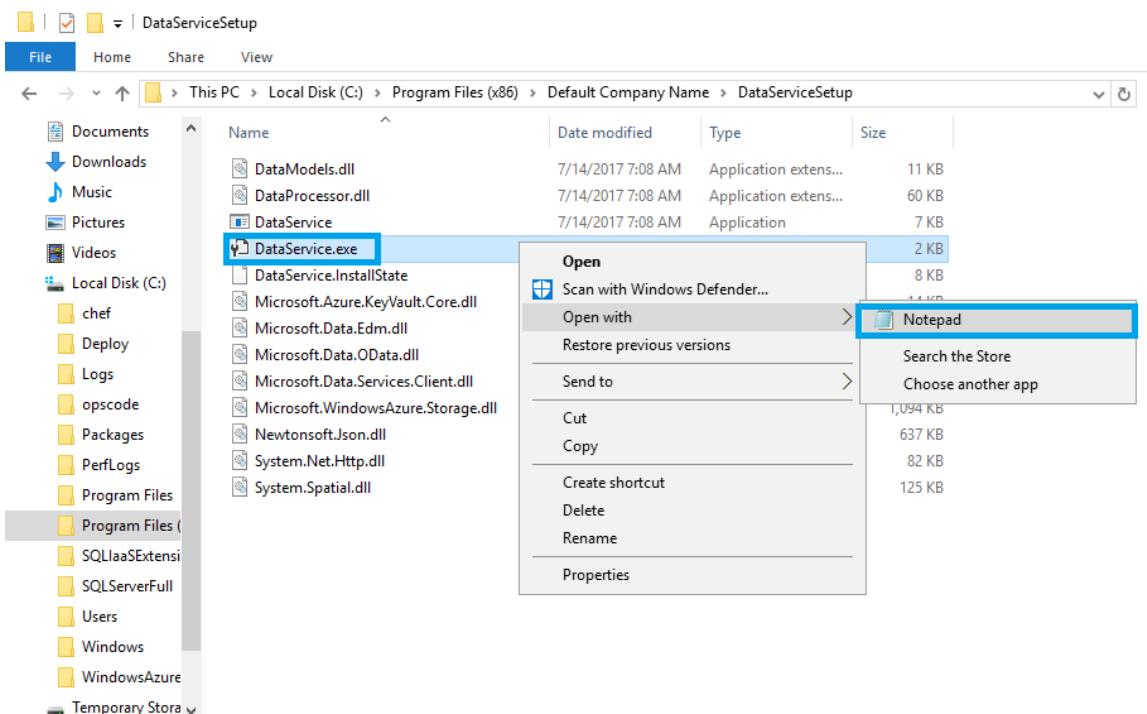
```

/*
***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [Id]
    ,[Weather]
    ,[TimeStamp]
    ,[Pressure]
    ,[Relative Humidity]
    ,[Temperature]
    ,[Visibility]
    ,[WindDirection]
    ,[Wind Speed]
    ,[PintSTicks]
    ,[PintShapeID]
FROM [PIBAView].[dbo].[Weather]

```

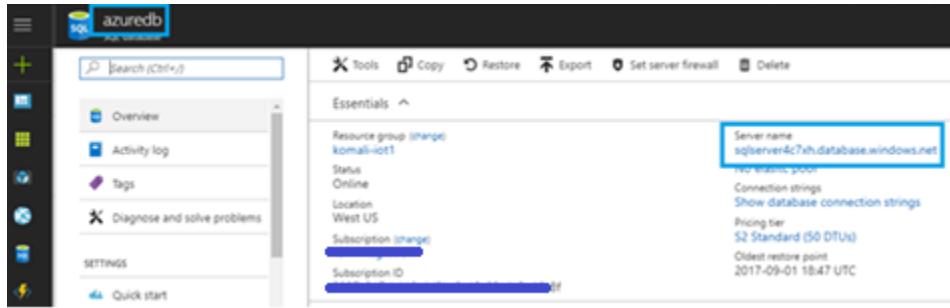
1	1	Weather	2017-08-24 04:44:07.980	30.7119654764943	67.7991369123567	74.0014907782904	6.77991369123567	Light Rain Fog/Mist
2	2	Weather	2017-08-24 04:45:07.870	28.8448272332758	21.1206808318946	46.4612016908178	2.11206808318946	Mostly Cloudy
3	3	Weather	2017-08-24 04:46:07.747	31.6321701387093	90.8042534677331	87.5745095459626	9.08042534677332	Thunderstorm Light Rain
4	4	Weather	2017-08-24 04:47:07.627	30.4195130441429	60.4878261035717	69.6878174011073	6.04878261035717	Fair and Windy
5	5	Weather	2017-08-24 04:48:07.497	29.2068594945764	30.1713887394103	51.801125262521	3.01173887394103	Overscast
6	6	Weather	2017-08-24 04:49:07.357	31.213458955575	80.336457388368	81.38865334594727	8.0386457388368	Heavy Rain
7	7	Weather	2017-08-24 04:49:42.220	31.9218162390971	98.0454059774269	91.8467859266818	9.80454059774267	Thunderstorm Light Rain
8	8	Weather	2017-08-24 04:50:07.187	29.220638415385	30.5015960384633	51.9959416626934	3.05015960384633	Fog/Mist
9	9	Weather	2017-08-24 04:50:42.107	30.7091591445306	67.728978132653	73.9600973818265	6.7728978132653	Light Rain Fog/Mist
10	10	Weather	2017-08-24 04:51:06.987	29.0107081799626	25.26771799052	48.9079536194484	2.526771799052	Partly Cloudy

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



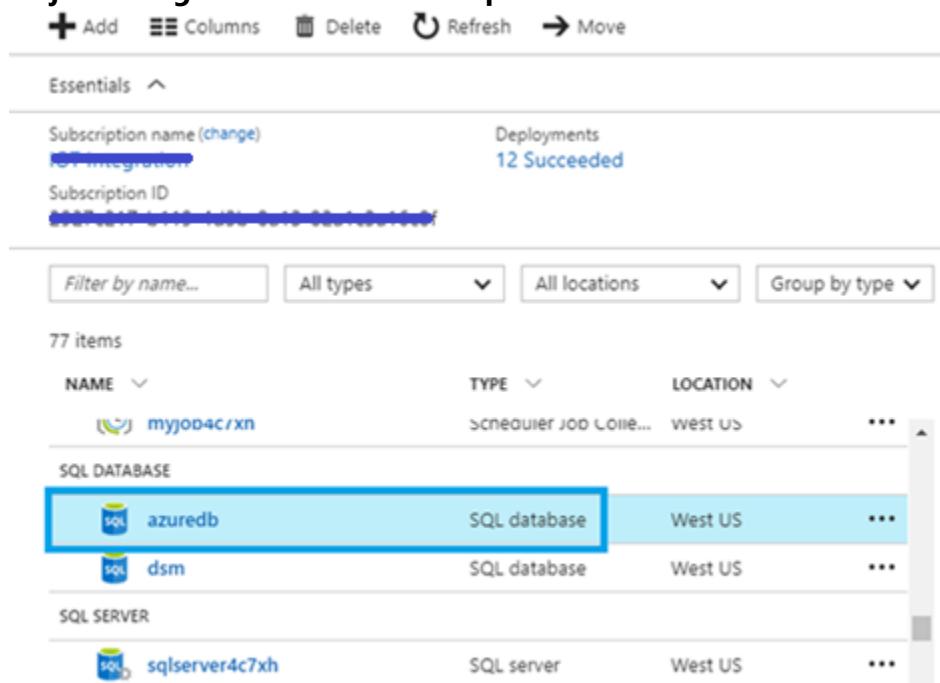
32. Before proceeding, you must update the values in azure connection string, Storage connection string, pi server connection string.

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**

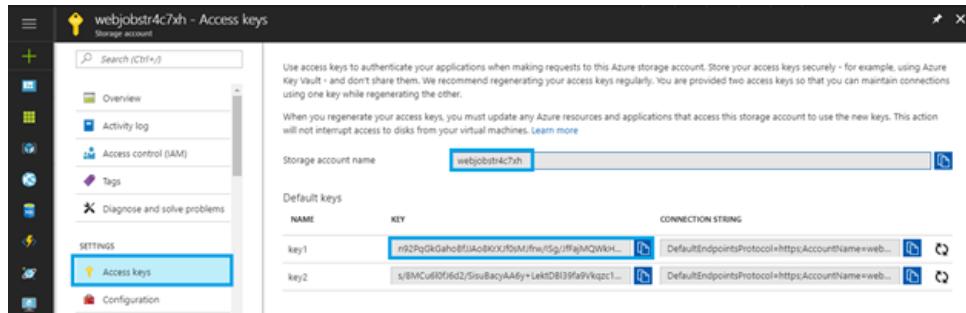


The screenshot shows the Azure portal interface for a database named 'azuredb'. The left sidebar has icons for Overview, Activity log, Tags, Diagnose and solve problems, SETTINGS, and Quick start. The main area shows 'Essentials' with details: Resource group (change), Status Online, Location West US, Subscription (change), and Subscription ID. A callout box highlights the 'Server name' field, which contains 'sqlserver4c7xh.database.windows.net'. Other options shown include 'No elastic pool', 'Connection strings', 'Show database connection strings', 'Pricing tier S2 Standard (50 DTUs)', and 'Oldest restore point 2017-09-01 18:47 UTC'.

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



The screenshot shows the Azure portal 'Subscriptions' blade. At the top, there are buttons for Add, Columns, Delete, Refresh, and Move. Below that is a search bar and filter options: Filter by name..., All types, All locations, and Group by type. The main area displays 77 items. It includes sections for NAME, TYPE, and LOCATION. Under 'NAME', it lists 'myjob04c/xn' (Scheduler Job Collection) and 'azuredb' (SQL database). Under 'TYPE', it lists 'SQL database' for both entries. Under 'LOCATION', it lists 'west US' for both. There are three dots for each entry. The 'azuredb' entry is highlighted with a blue box.



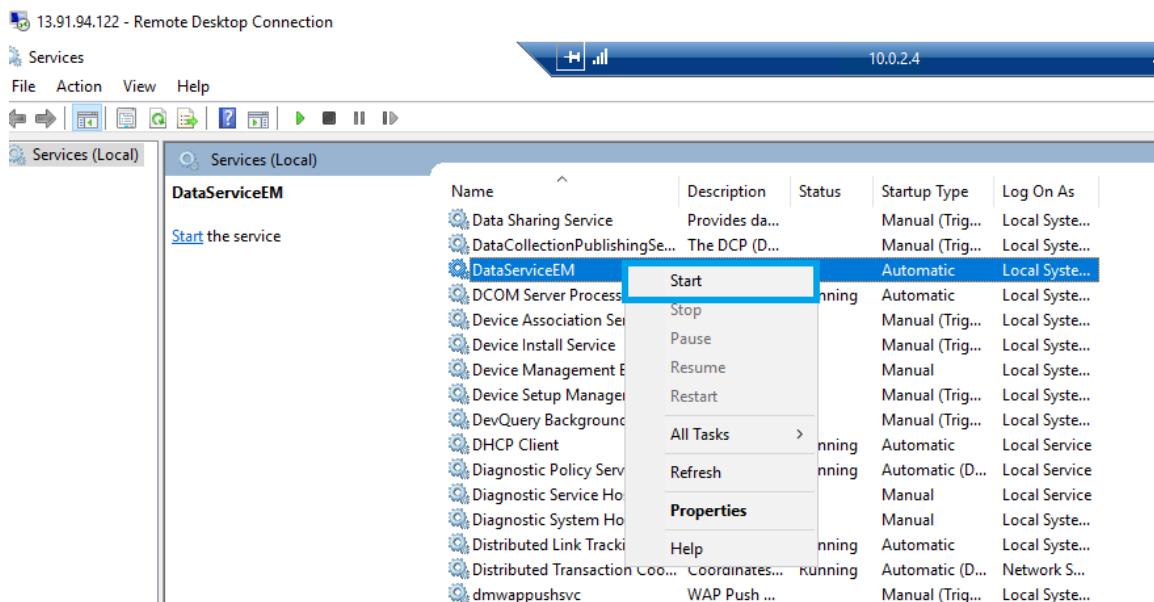
Pi Connection String: Set the **data source** as the AF server name, **Initial catalog** as created database name in AF server which you created in PI system explorer, and the id/password as the ones used to login the SQL studio.

```

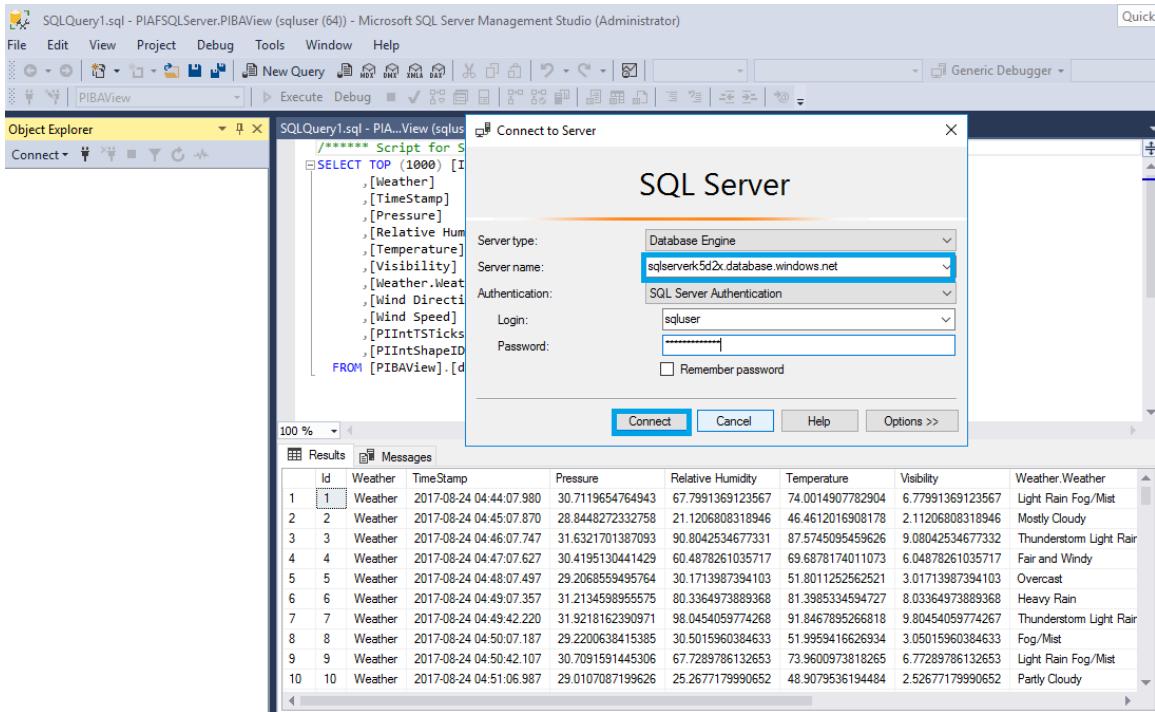
File Edit Format View Help
<xml version="1.0" encoding="utf-8">
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <appSettings>
    <add key="PiServer" value="PiServer1" />
    <add key="AzureConnectionString" value="Server=tcp:sqlserver4c7xh.database.windows.net,1433;Initial Catalog=azuredb;Persist Security Info=False;User ID=sqlluser;P<!-->
    <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=webjobstr4c7xh;AccountKey=n92PqGkGaho8fIAo8dXJfbMlfrwHsgJfRjMQwKH...<!-->
    <add key="PiServerConnectionString" value="data source=PIAFSQLServer;initial catalog=PIBAView;persist security info=True;user id=sqlluser;password=P@ssw0rd1234" />
  </appSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6eed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0-10.0.0.0" newVersion="10.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>

```

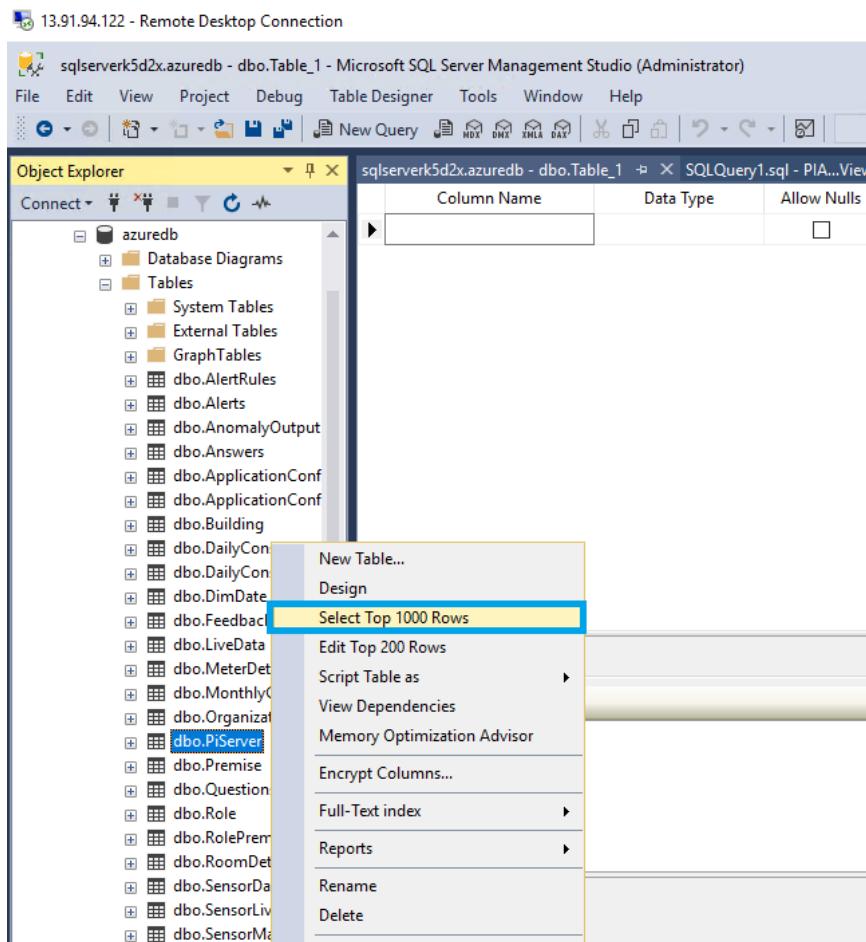
- After updating the values in the data service.exe files, navigate **Start > Service** to start the **DataServicesEM**.



34. 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**.



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



36. Check the updated table.

The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left shows the database structure for 'azuredb'. The central pane displays a query results grid for the 'PiServer' table. The query is:

```

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

```

The results grid shows one row:

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

The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left shows the database structure for 'azuredb'. The central pane displays a query results grid for the 'liveidata' table. The query is:

```

select * from liveidata

```

The results grid shows two rows:

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

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

File Edit View Query Project Debug Tools Window Help

azuredb Execute Debug

Object Explorer

Connect ▾

azuredb

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 (saluser (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 Execute Debug

Object Explorer

Connect ▾

azuredb

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 (saluser (115))*

SQLQuery2.sql - sql...redb (saluser (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

37. 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.

Microsoft Azure Resource groups > ooha-iot > sqlserverk5d2x - Firewall / Virtual Networks (Preview)

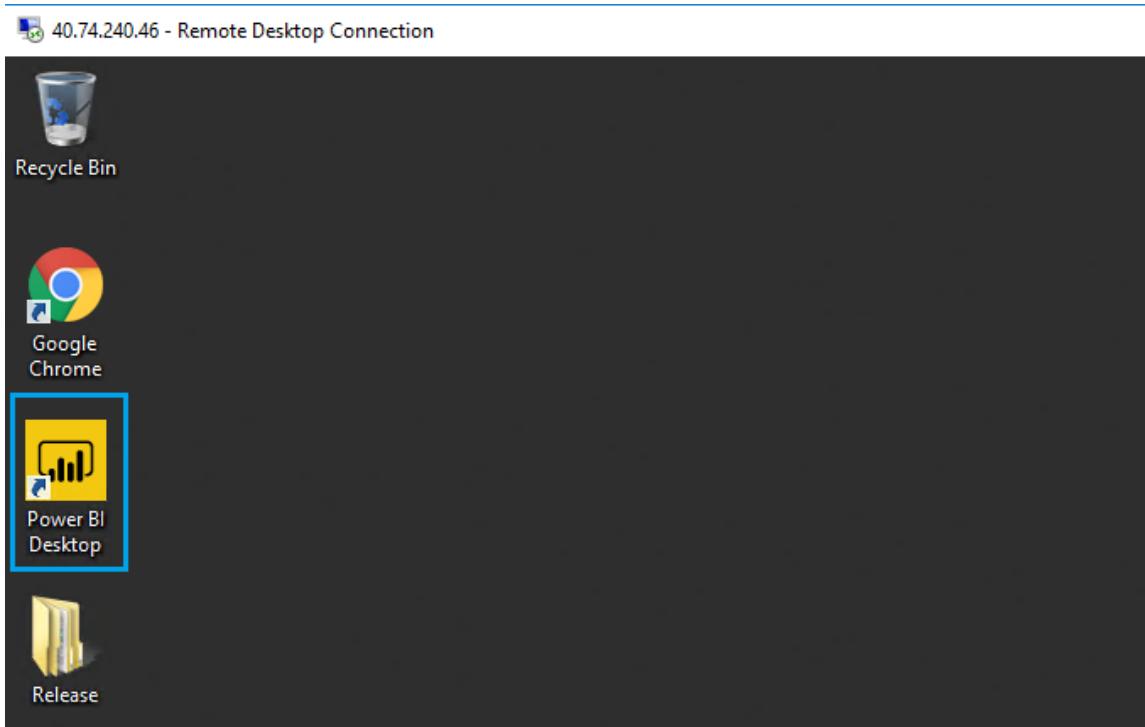
sqlserverk5d2x - Firewall / Virtual Networks (Preview)

Save Discard + Add client IP + Add VNET rule

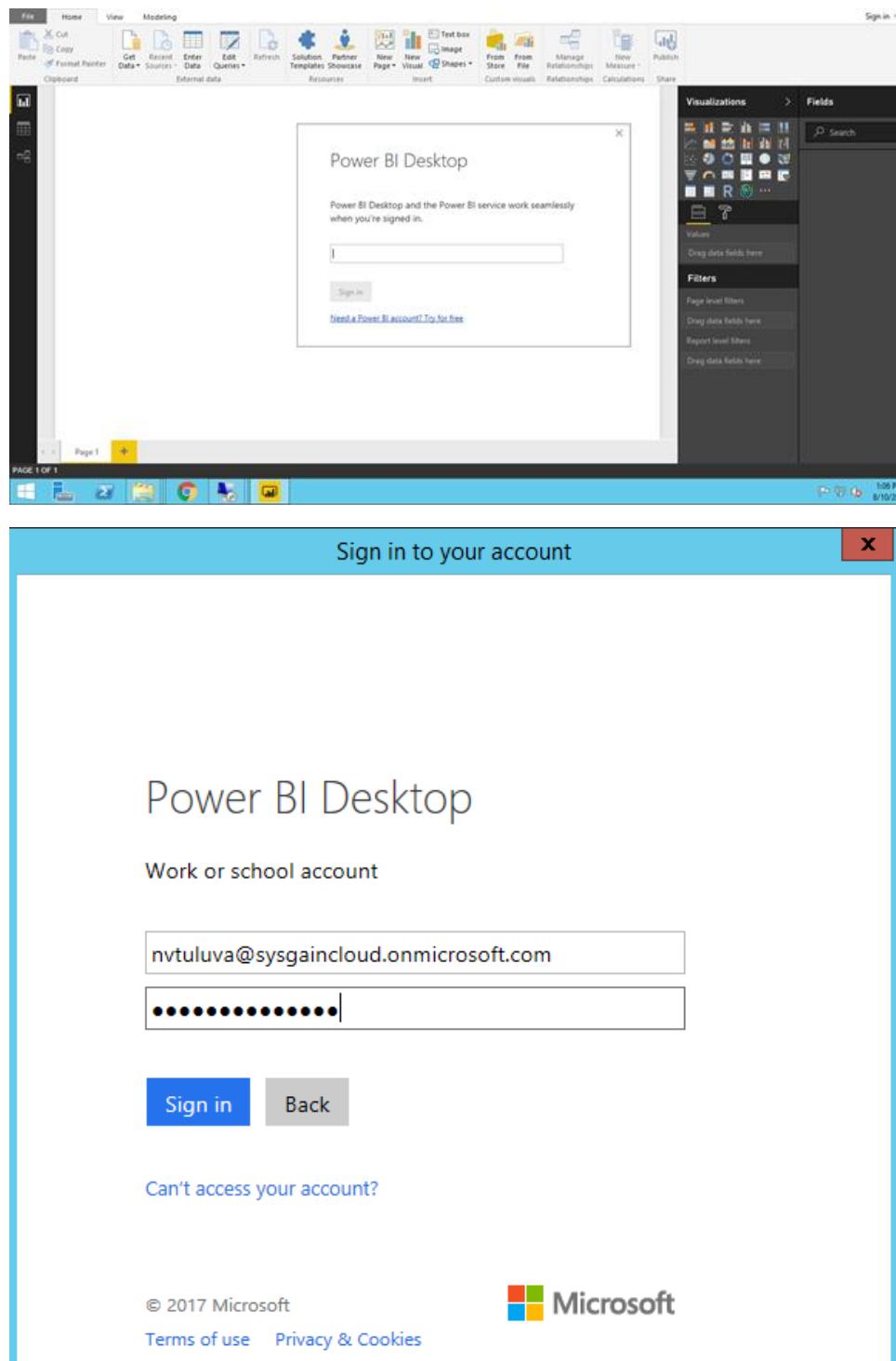
Connections from the IPs specified below provides access to all the databases in sqlserverk5d2x.

RULE NAME	START IP	END IP	...
firewall	13.91.94.122	13.91.94.122	...

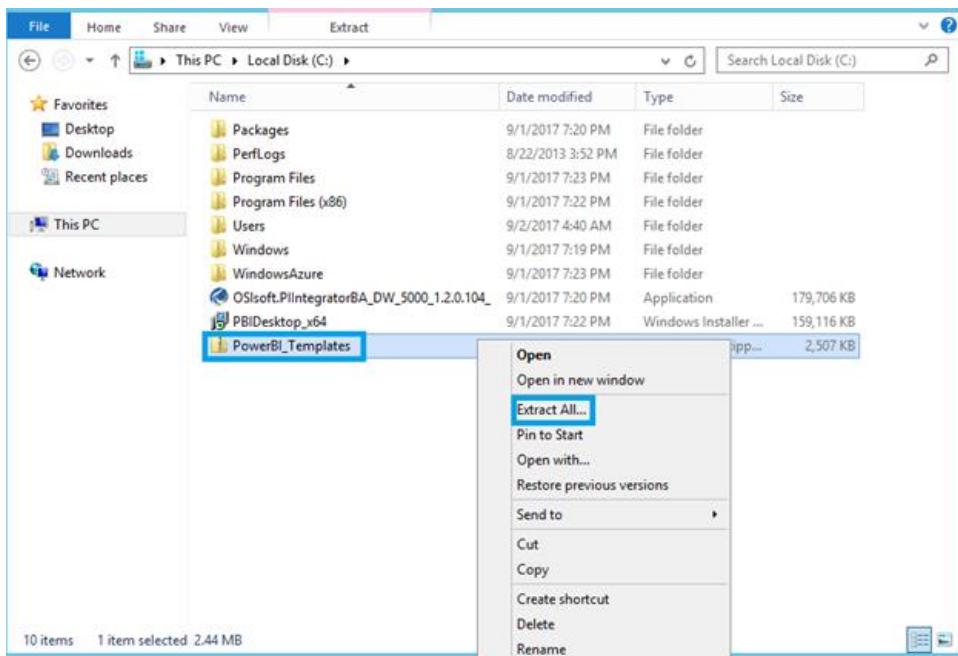
38. Login to the Bastionserver you can see the power BI desktop in Bastionserver desktop, Click on that Power BI desktop.



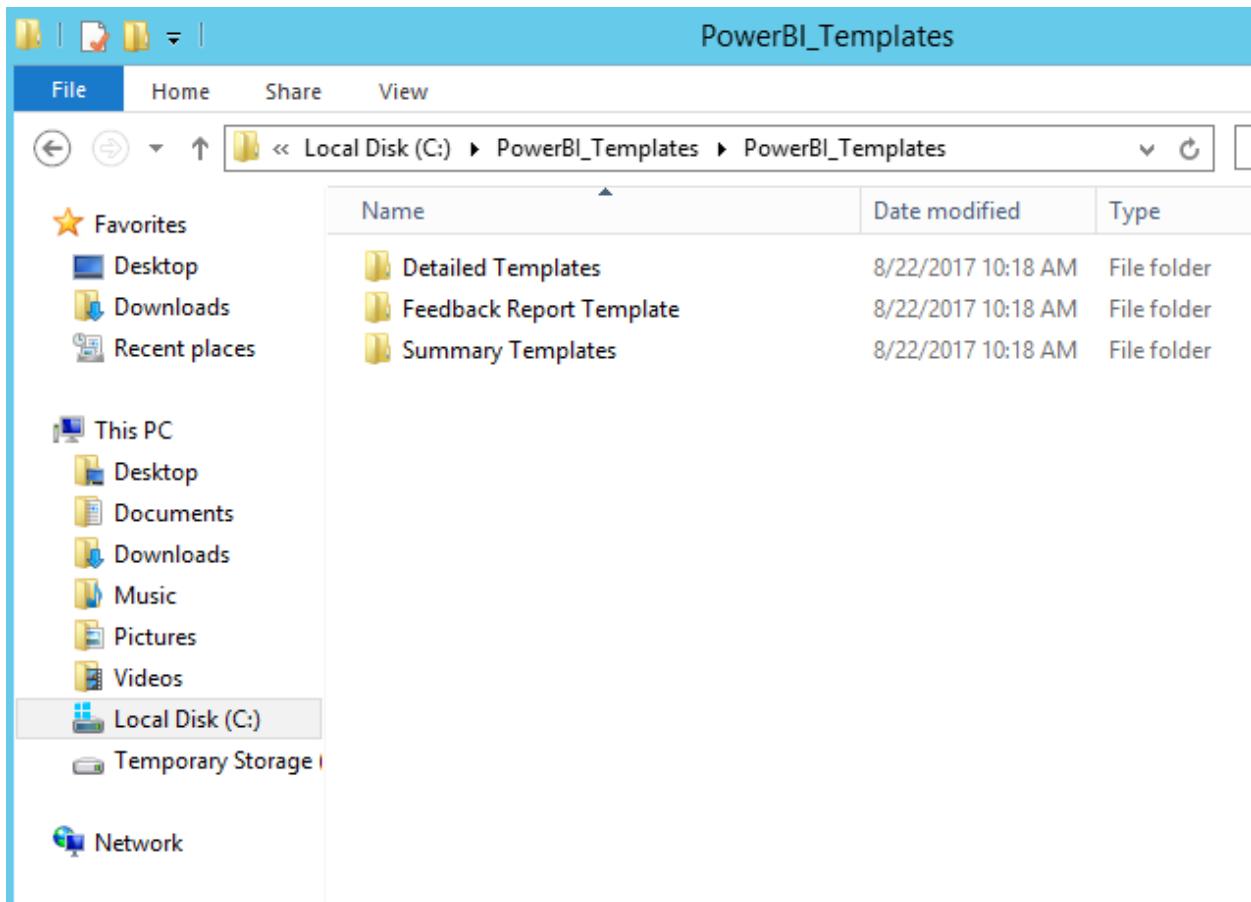
39. Log in with the same credentials used while registration of webapp with power BI you don't need to create a power BI account.



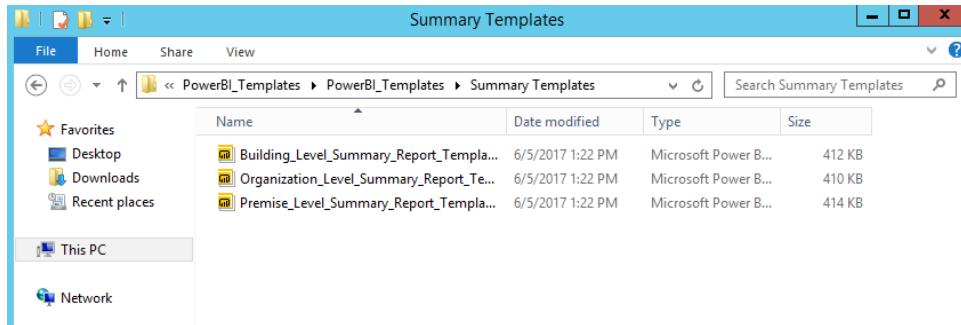
40. In Bastion server, navigate to **Local disk (C:) > unzip the Power Bi templates > Power Bi templates**.



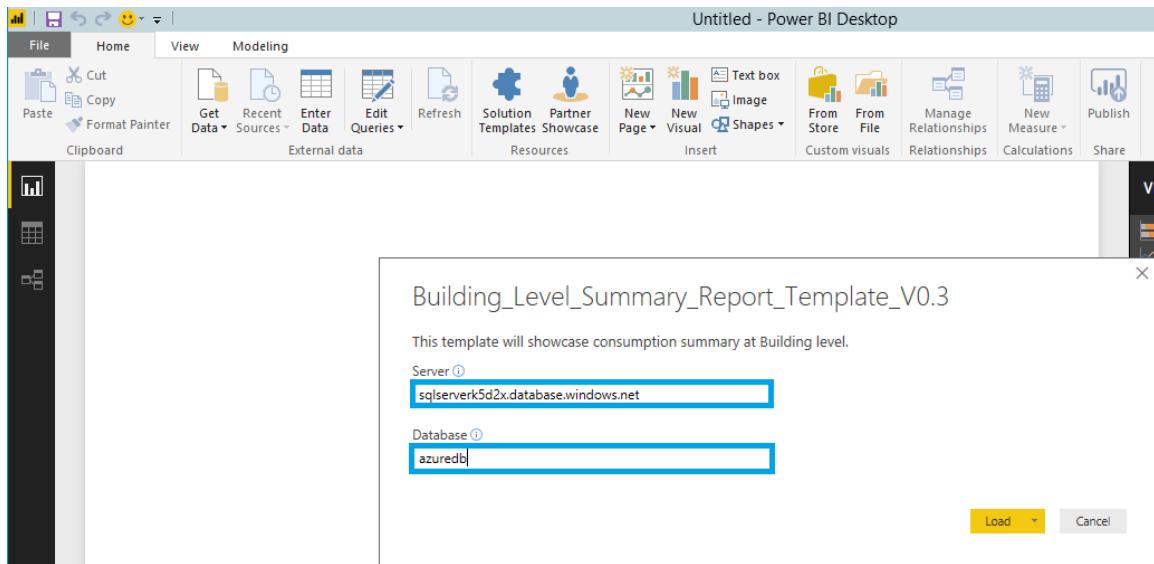
41. You can view Power Bi templates in the Local disk (C :)



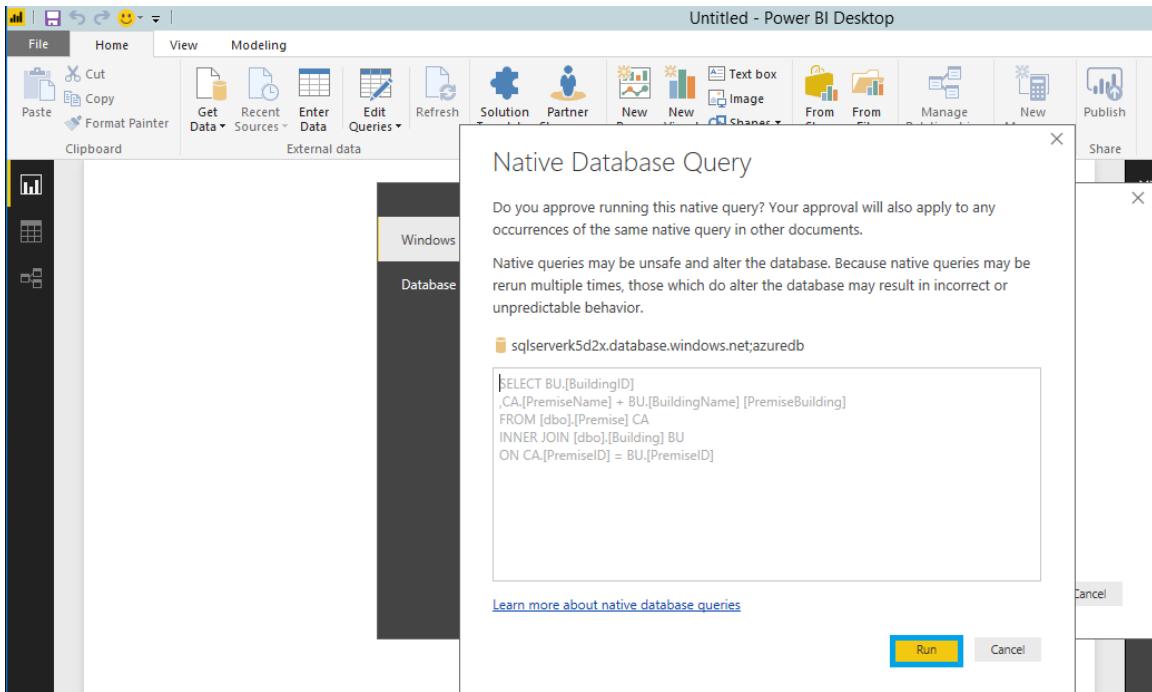
42. Navigate to the summary templates folder, click on “**Building_level_summary_templates**” click on keep using Microsoft Power BI Desktop



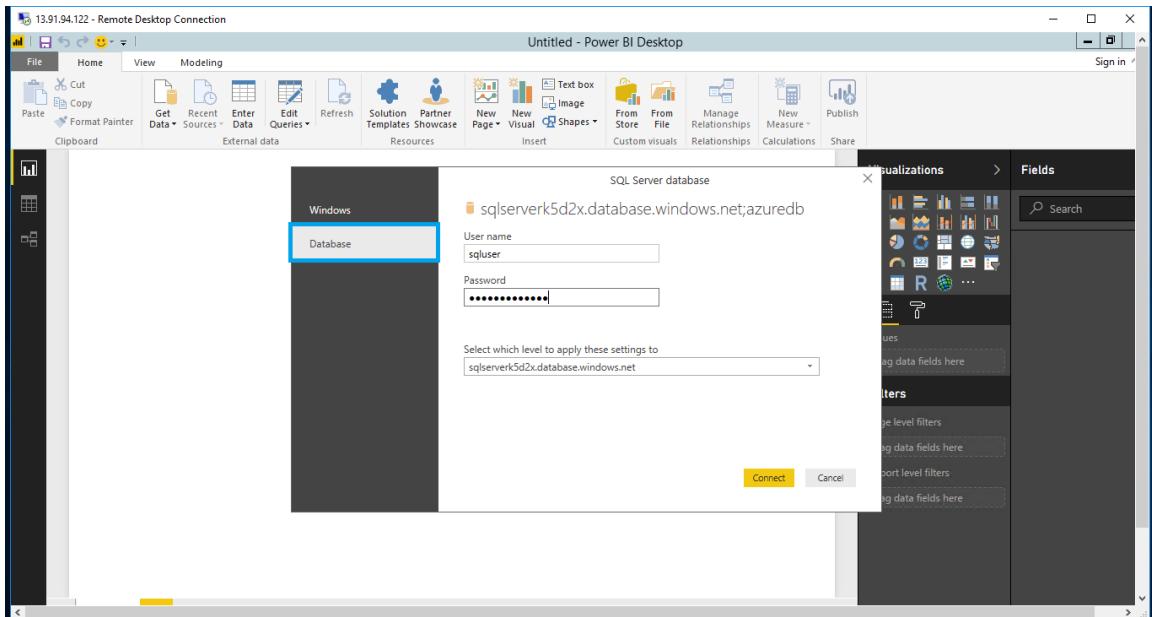
43. It prompts for power BI server and database details, provide you're Azure SQL server name and azure SQL database name from your deployed azure SQLServer .and click on **Load**.



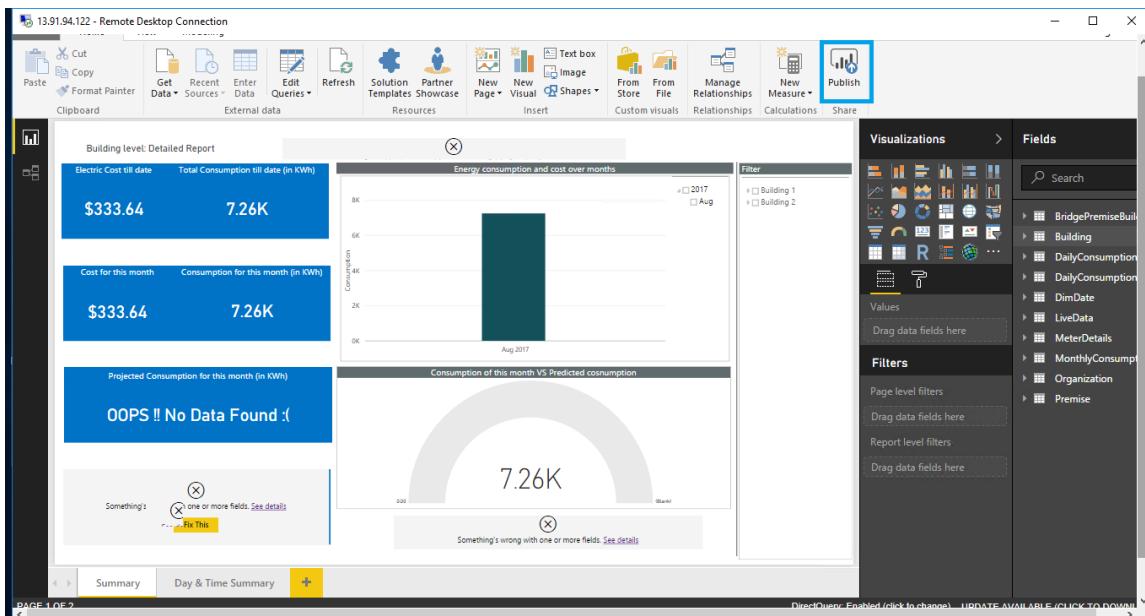
44. Once you click on Load , the “Native Database Query” will appear click on **Run**.



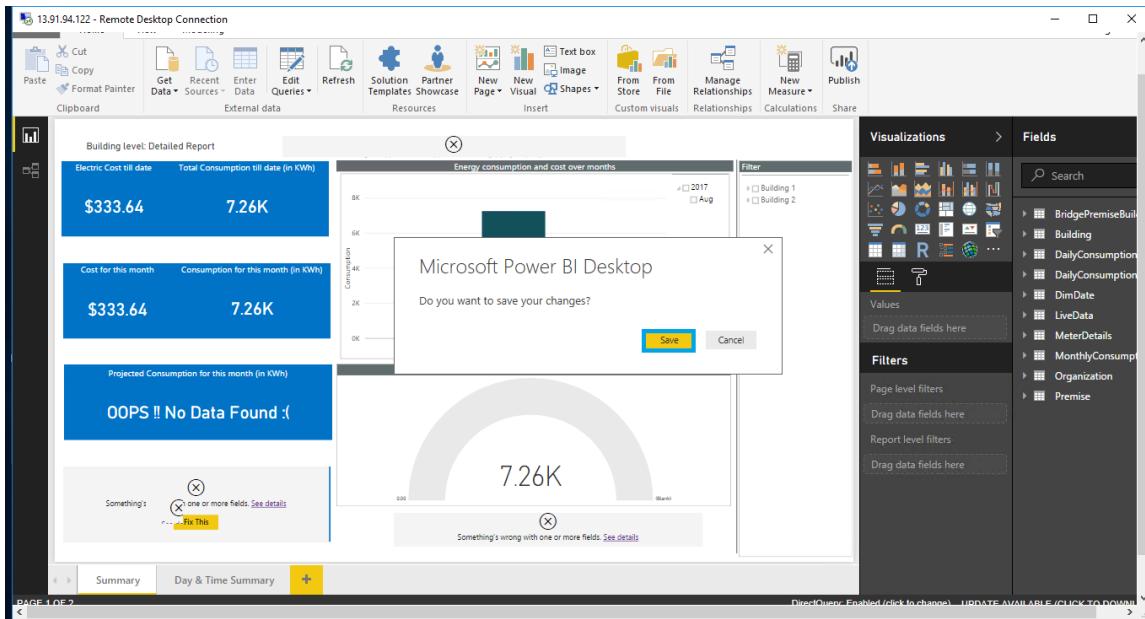
45. Select **Database** after connecting to the Azure SQL Server. Enter the login credentials of Azure database and click on **Connect**.



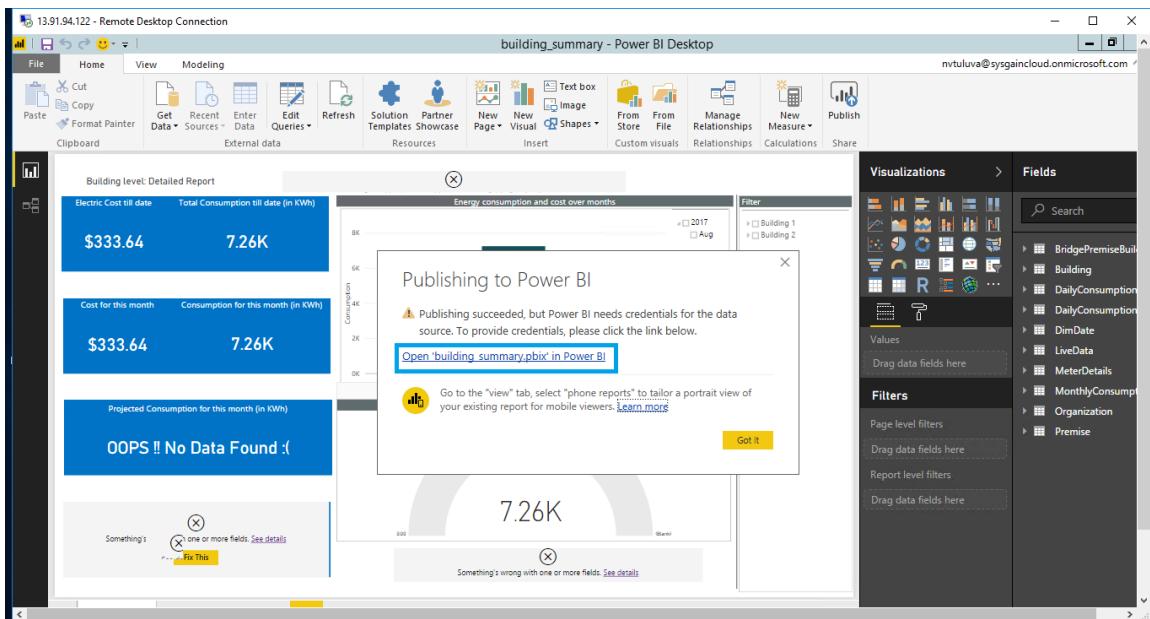
46. Click on **Publish**.



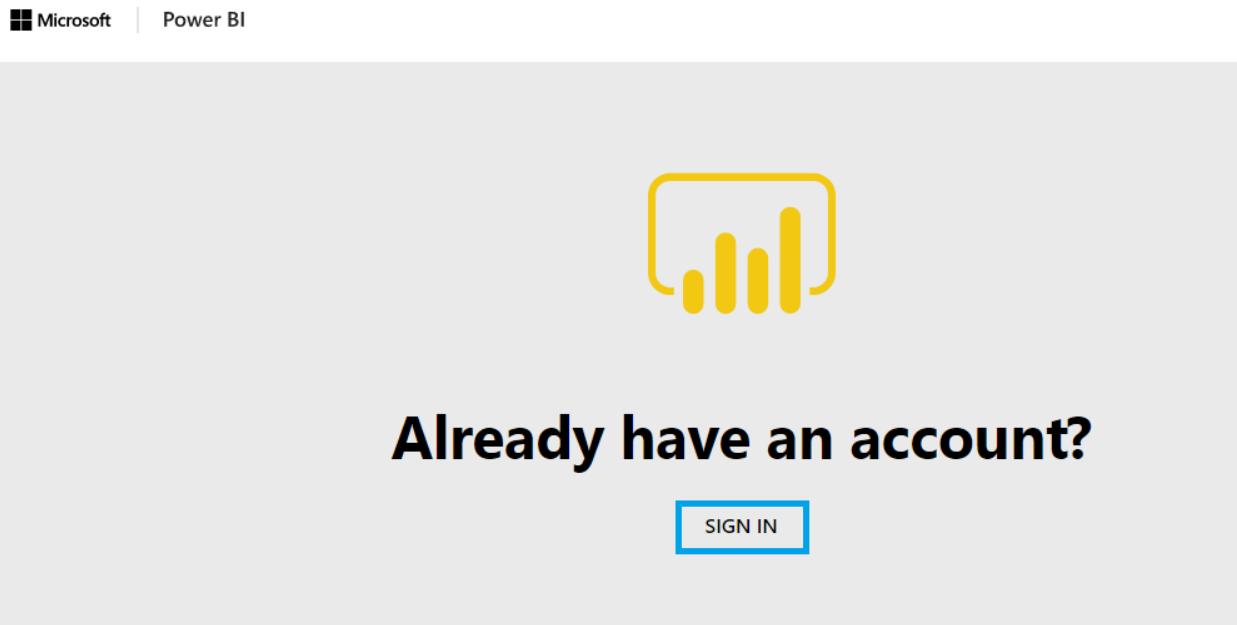
47. Save the changes.



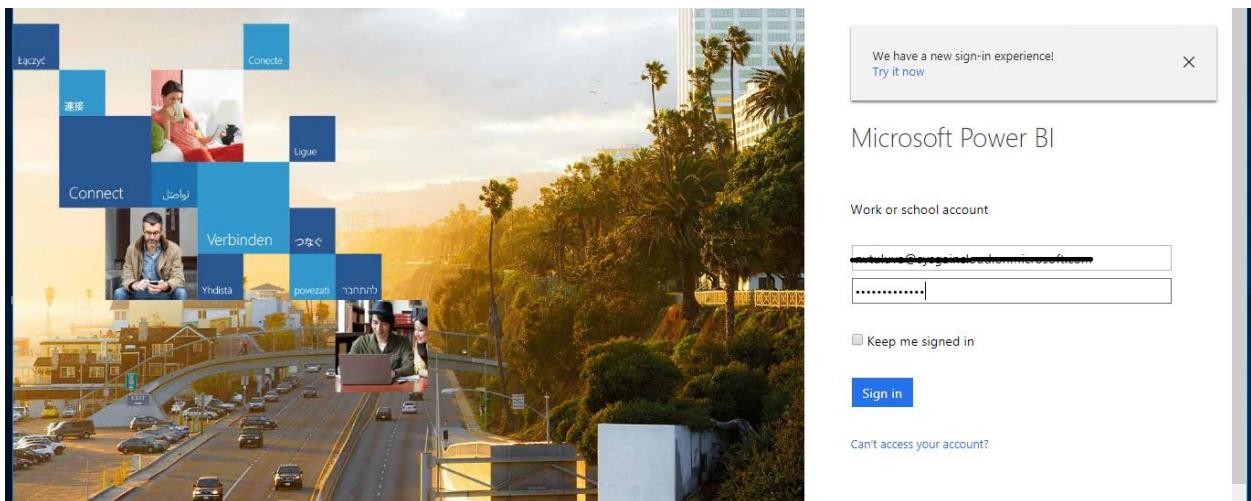
48. Click on the link as shown below, it will open in a web browser.



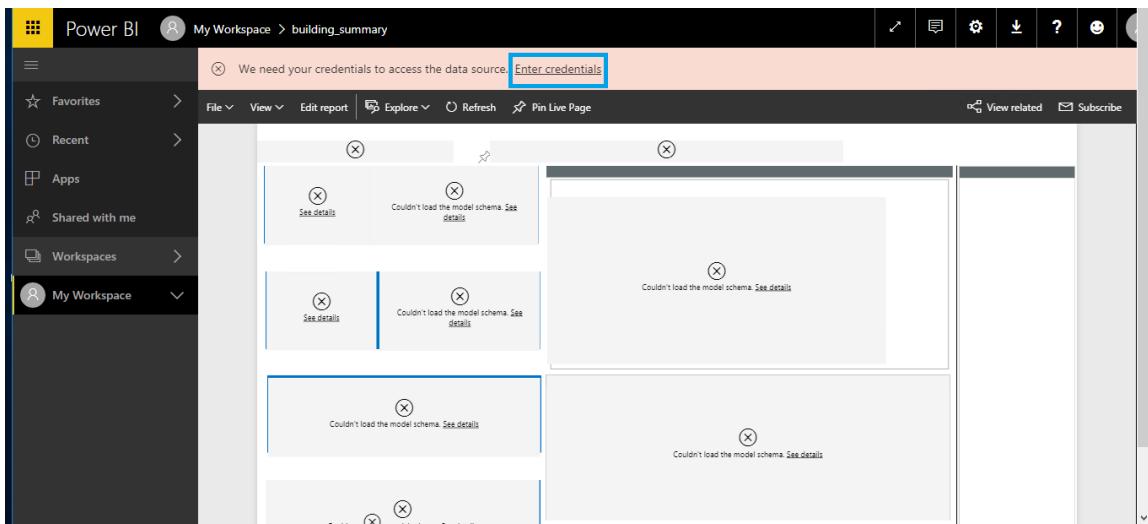
49. Sign in with the same credentials which were used to log to Power BI.



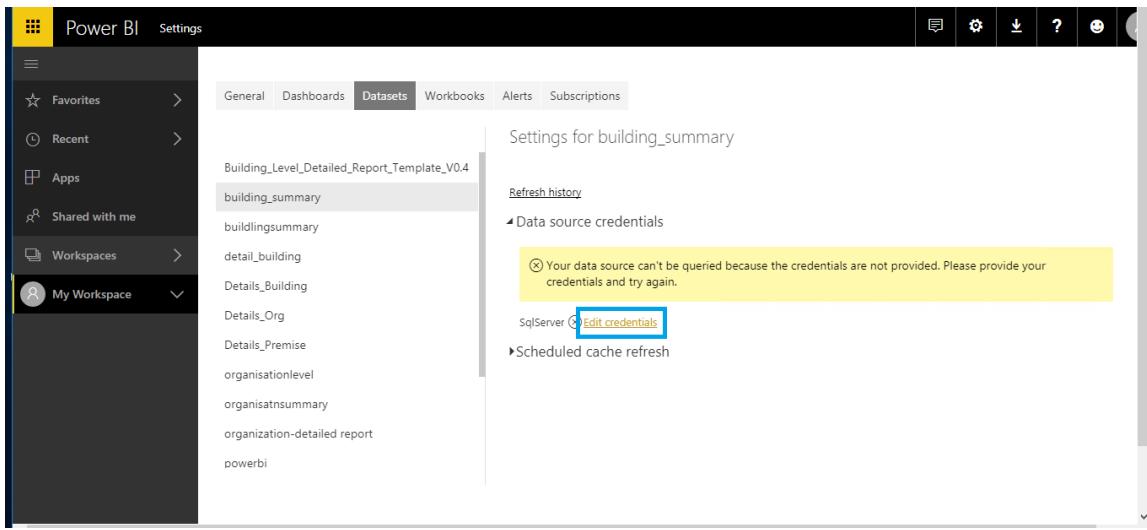
50. Enter the Power BI Credentials.



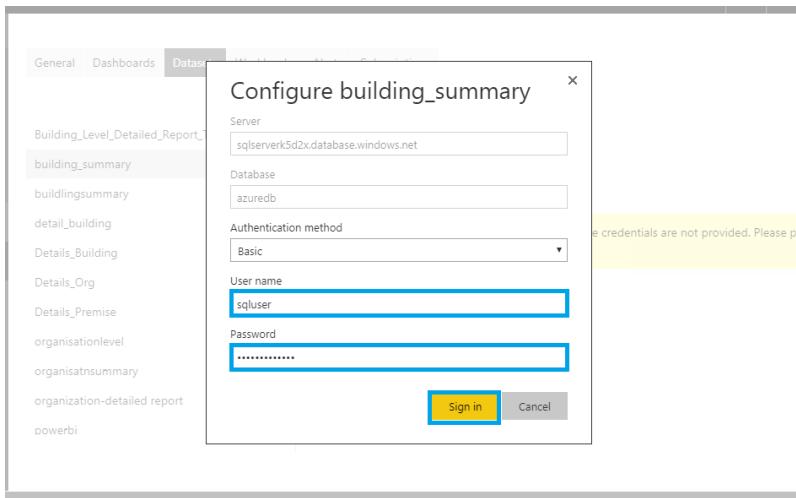
51. Click on Enter credentials.



52. Click on **Edit credentials**.



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



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

The screenshot shows a Power BI workspace interface. On the left, there's a sidebar with navigation options like Favorites, Recent, Apps, Shared with me, Workspaces, and My Workspace. The 'My Workspace' section is highlighted with a blue box. Under 'Workspaces', 'Smmry_Building' is also highlighted with a blue box. The main area displays a 'Building level: Detailed Report' for 'Smmry_Building'. It includes several cards: '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), a bar chart titled 'Energy consumption and cost over months' showing consumption for Aug 2017 (approx. 8K), a gauge titled 'Consumption of this month VS Predicted consumption' showing 8.10K, and two error messages: 'OOPS !! No Data Found :(' under 'Projected Consumption for this month (in kWh)' and 'Projected cost for this month'.

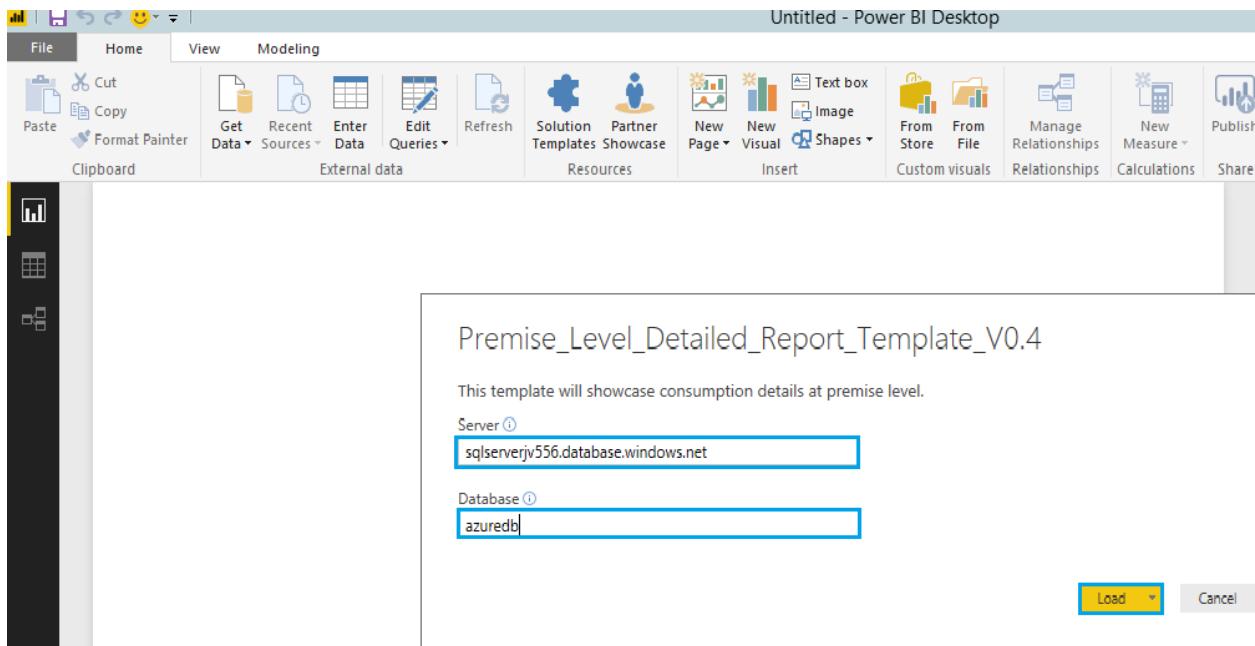
55. Similarly, follow the same process for Organisation and Premise Summary templates.

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

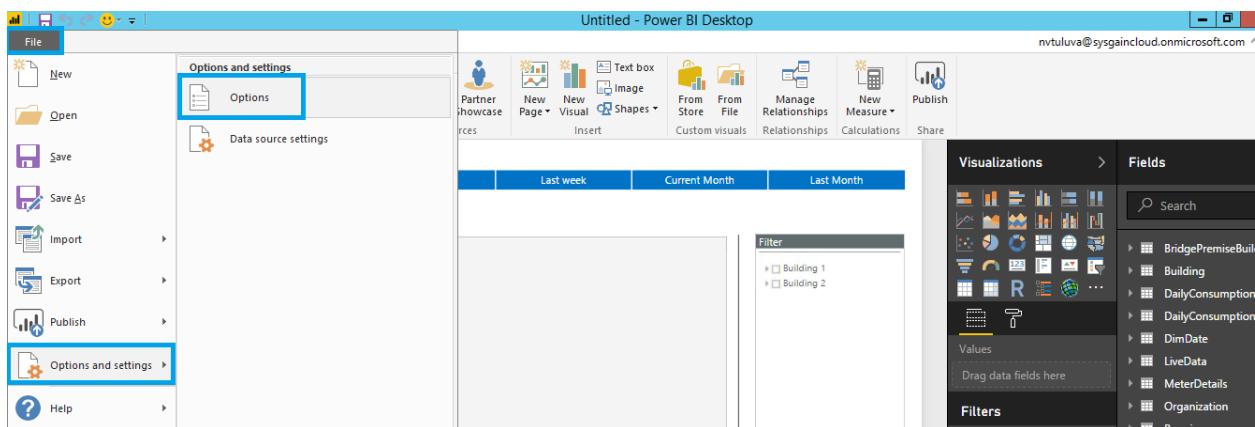
The screenshot shows a Windows File Explorer window titled 'Detailed Templates'. The top navigation bar includes File, Home, Share, View, and a tab labeled 'Detailed Templates'. The address bar shows the path: This PC > Local Disk (C:) > PowerBI_Templates > PowerBI_Templates > Detailed Templates. The left sidebar has links for Favorites, Desktop, Downloads, and Recent places, with 'This PC' selected. The main pane displays a table of files:

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

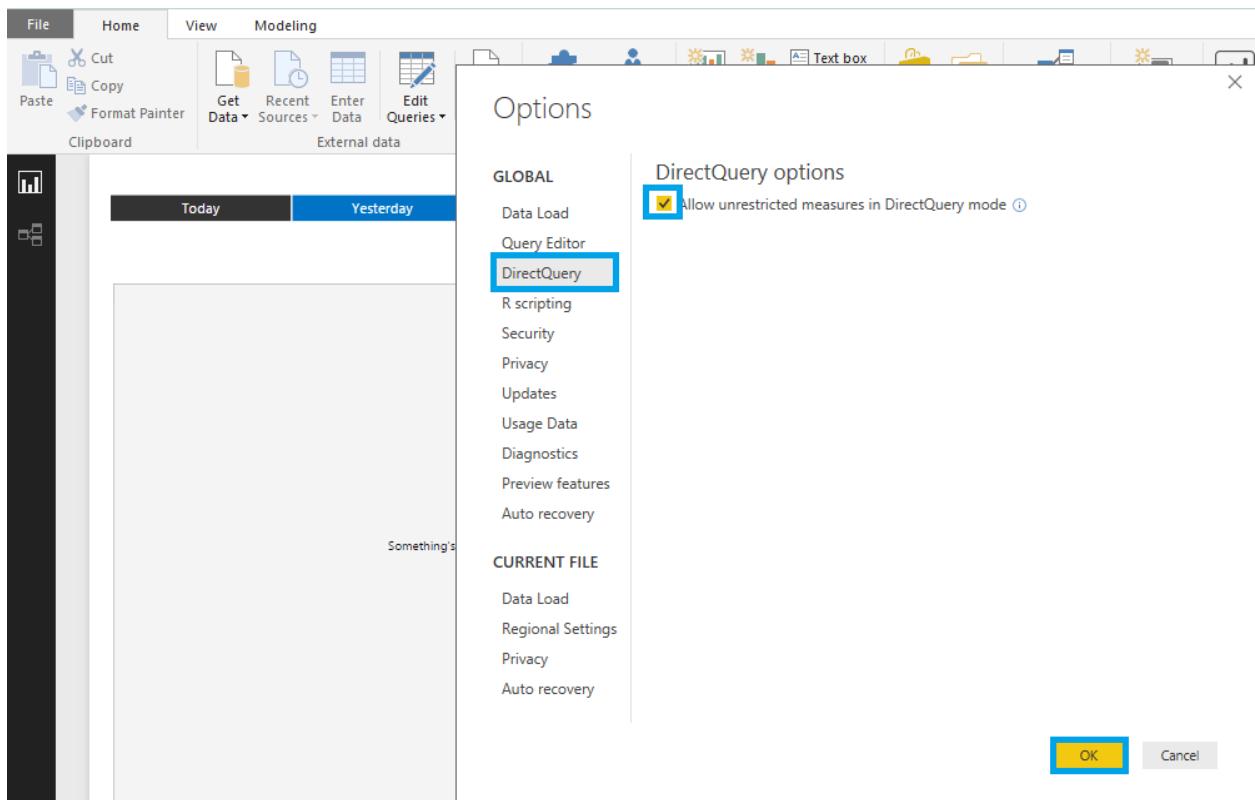
57. Enter the Azure SQL Server name with its password.



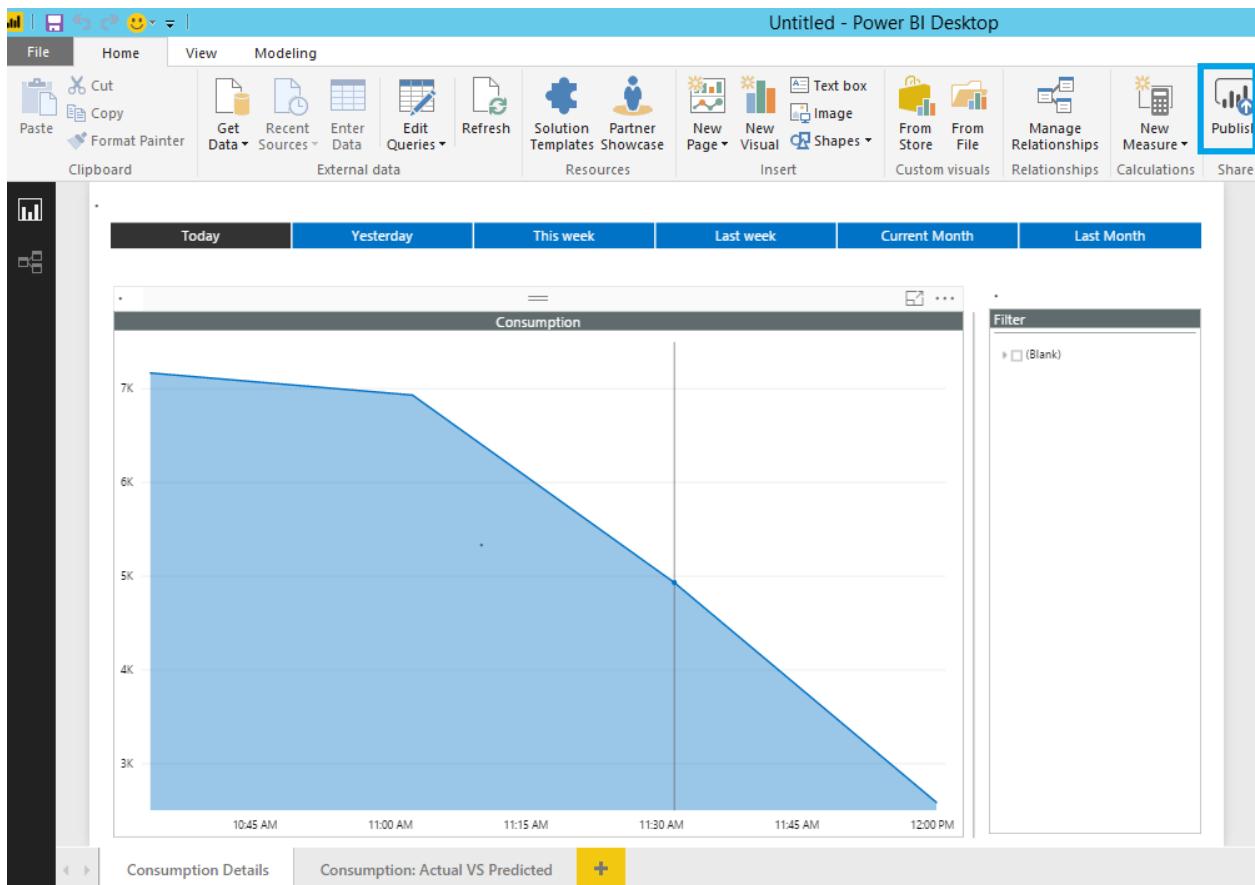
58. Navigate to **File > Options and Settings > Options**.



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



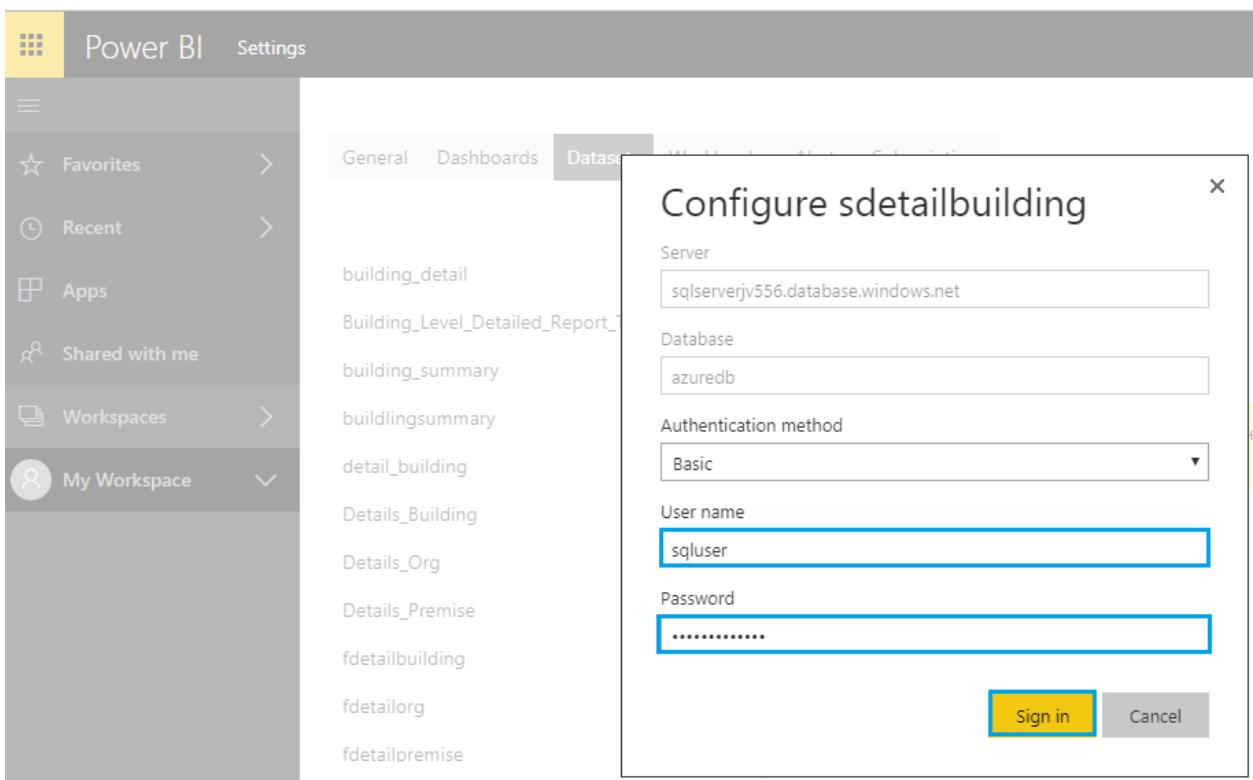
60. Click on **Publish** when you view the graph.



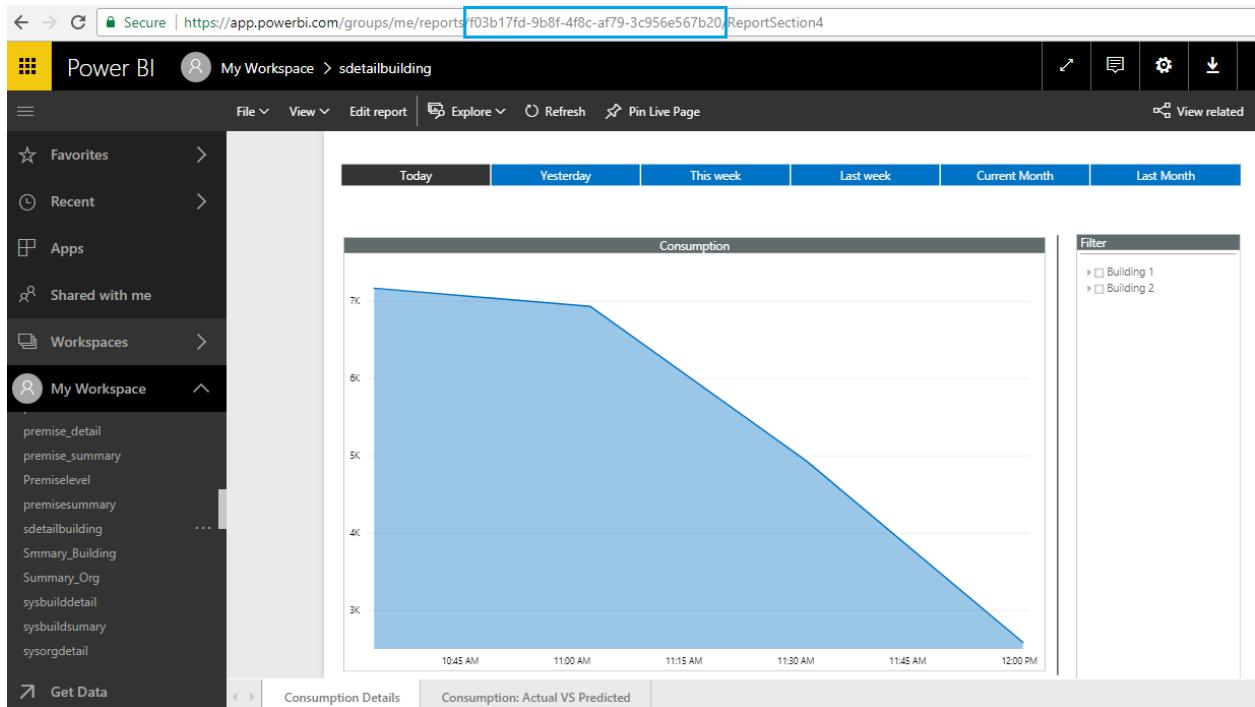
61. Click on **Enter credentials**.

The screenshot shows the Power BI web interface at the URL <https://app.powerbi.com/groups/me/reports/f03b17fd-9b8f-4f8c-af79-3c956e567b20/ReportSection4>. The left sidebar shows "Power BI", "My Workspace > sdetailbuilding", and navigation links for "Favorites", "Recent", "Apps", "Shared with me", "Workspaces", and "My Workspace". The main area displays a message: "We need your credentials to access the data source." with a blue-bordered button labeled "Enter credentials".

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



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



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

11. Configuring And Accessing The Webapp

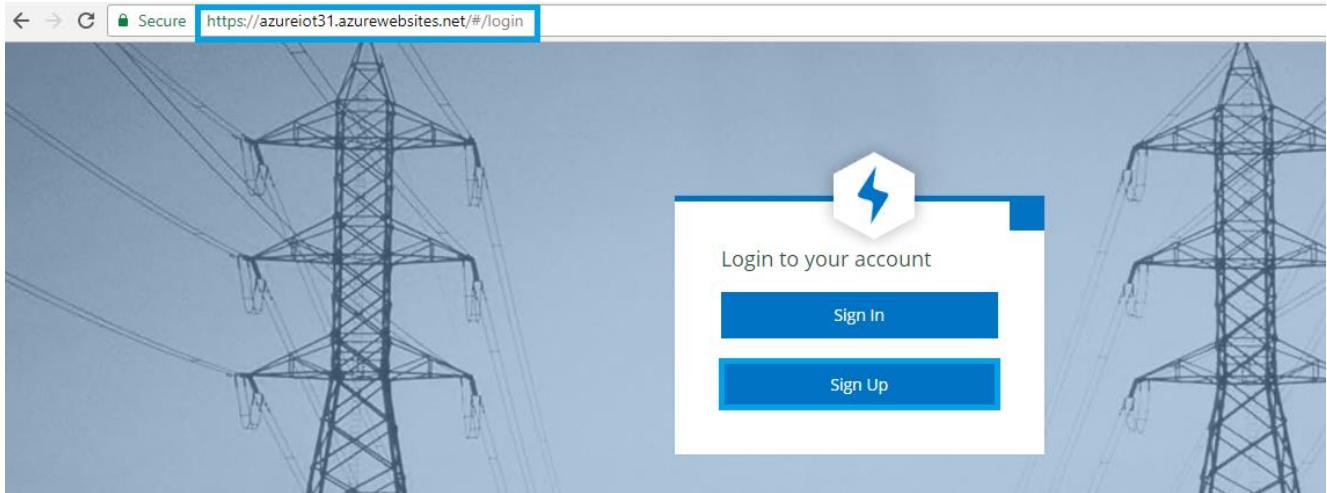
1. Go to the Web Application in the Resource Group and copy the "**URL**".

The screenshot shows the Azure portal interface for the 'iotnewappptest' App Service. The left sidebar has a green plus icon and several icons for monitoring and deployment. The main area is titled 'Overview' and contains the following details:

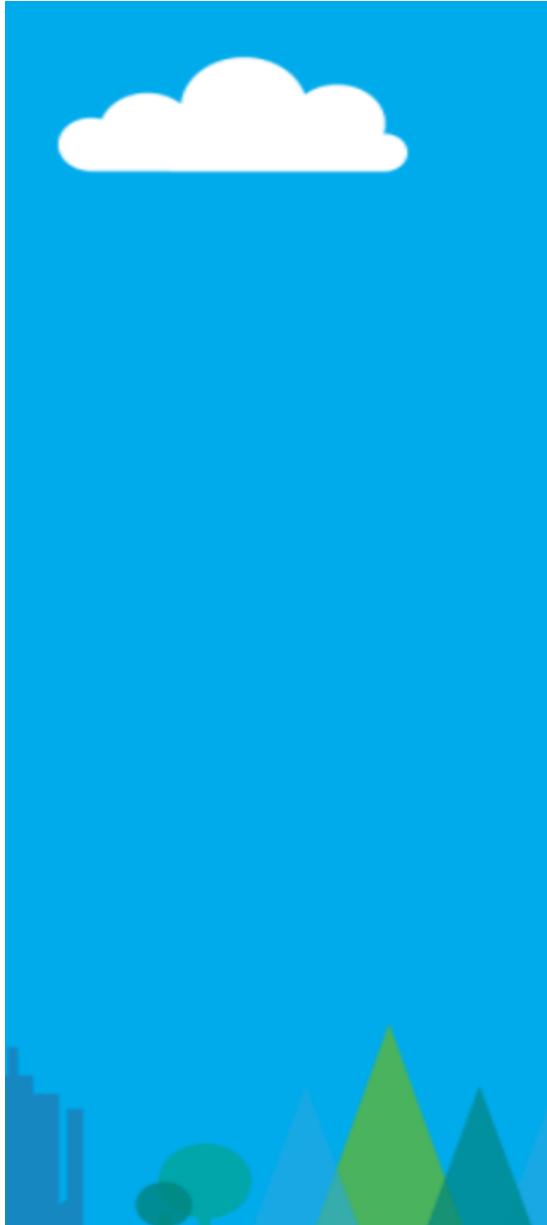
- Resource group (change):** [REDACTED]
- Status:** Running
- Location:** West US
- Subscription (change):** [REDACTED]
- Subscription ID:** [REDACTED]

On the right, there are three sections: 'Http 5xx' (100), 'Data In' (12kB), and 'Data Out' (4kB). At the top, there are buttons for 'Browse', 'Stop', 'Swap', 'Restart', 'Delete', 'Get publish profile', and 'Reset publish profile'.

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 have click on account sign up
4. Click on **Sign Up** to access the Webapp. 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

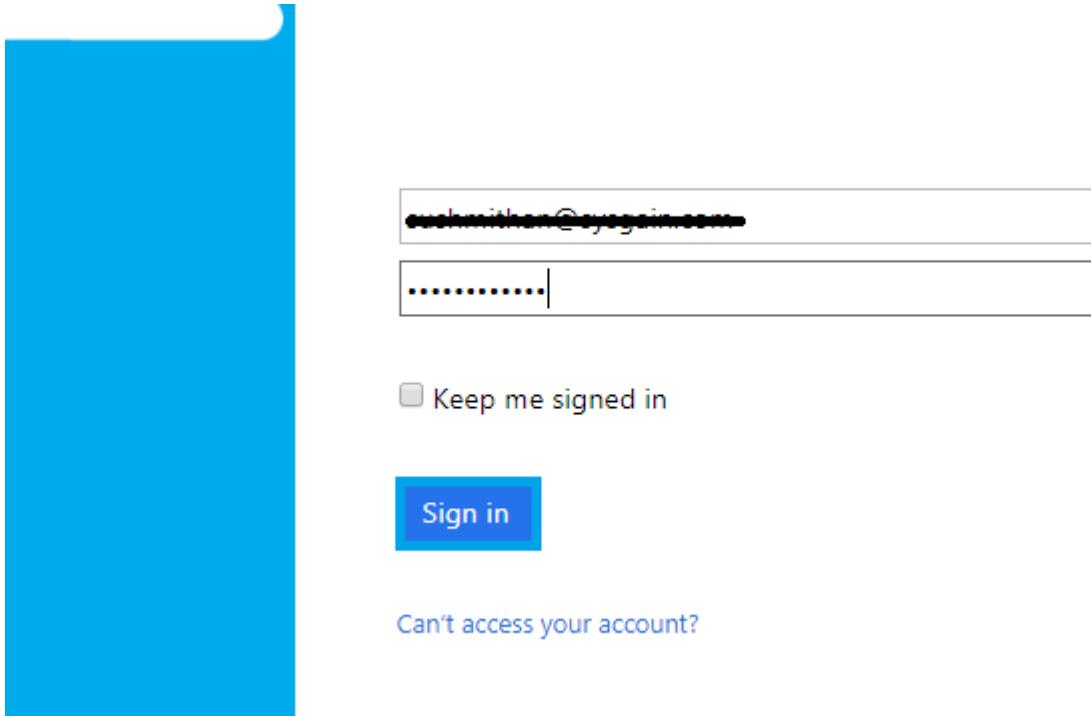
Display Name

Country/Region
 ▾

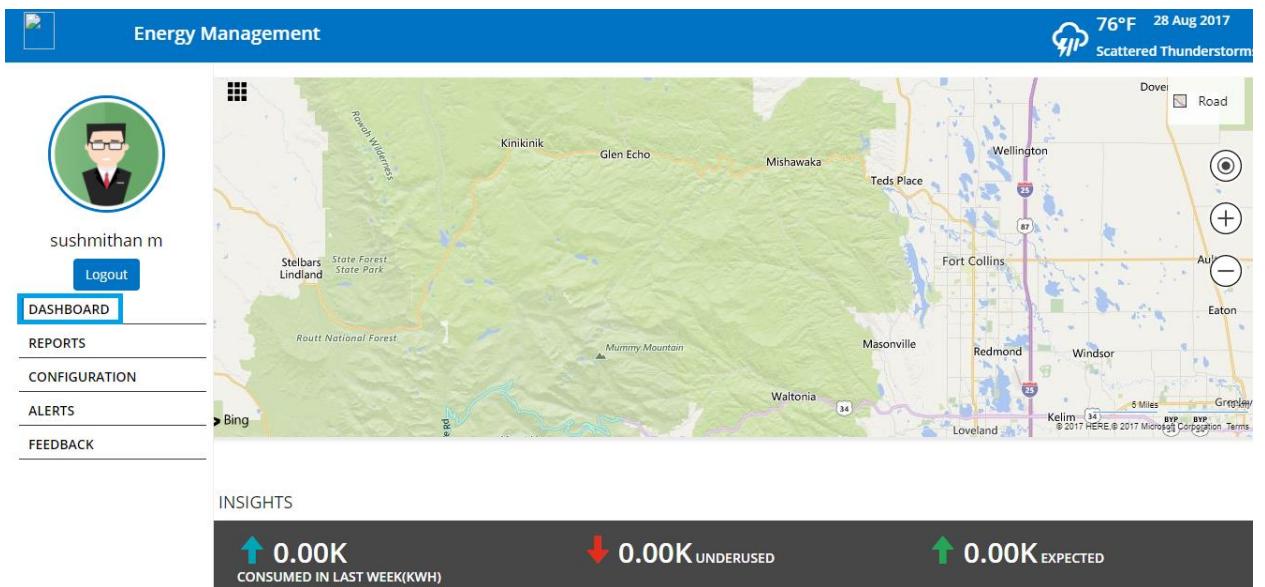
City

Activate Windows
Go to Settings to activate Windows.

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



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



- 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, the name "sushmithan m", a "Logout" button, and a navigation menu with options: DASHBOARD, REPORTS, CONFIGURATION (which is highlighted in blue), ALERTS, and FEEDBACK. The main content area has a title "Energy Management" and a section titled "Power BI Configuration(Organisation)". Below this, there are two tabs: "Power BI Configuration(Premise)" and "Power BI Configuration(Building)". A large input field contains two URLs: "https://app.powerbi.com/reportEmbed?reportId=c440389c-e9db-4733-b541-fc1f4d08f116" and "https://app.powerbi.com/reportEmbed?reportId=f03b17fd-9b8f-4f8c-af79-3c956e567b20". To the right of these URLs is a blue "Add" button. At the bottom of the configuration section is another tab labeled "Power BI Configuration(Feedback)".

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

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

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

The screenshot shows the Energy Management application interface, similar to the previous one but with different configuration tabs. The sidebar and main layout are identical. The main content area has a title "Energy Management" and a section titled "Power BI Configuration(Organisation)". Below this, there are two tabs: "Power BI Configuration(Premise)" and "Power BI Configuration(Building)". A large input field contains two URLs: "https://app.powerbi.com/reportEmbed?reportId=48bbe94e-a82a-4cfb-820e-8e66c83c2501" and "https://app.powerbi.com/reportEmbed?reportId=076c4c08-22c9-4e51-8c0a-13b10beb4695". To the right of these URLs is a blue "Add" button. Below these tabs are two more tabs: "Power BI Configuration(Premise)" and "Power BI Configuration(Building)".

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

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

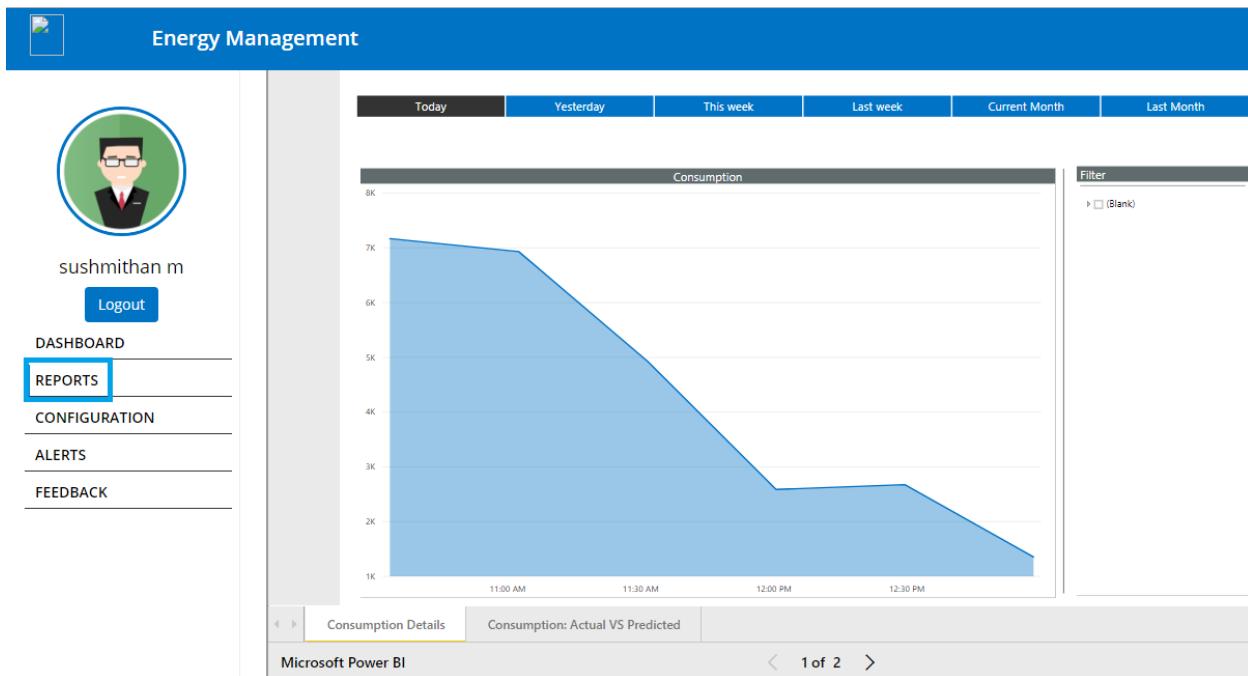
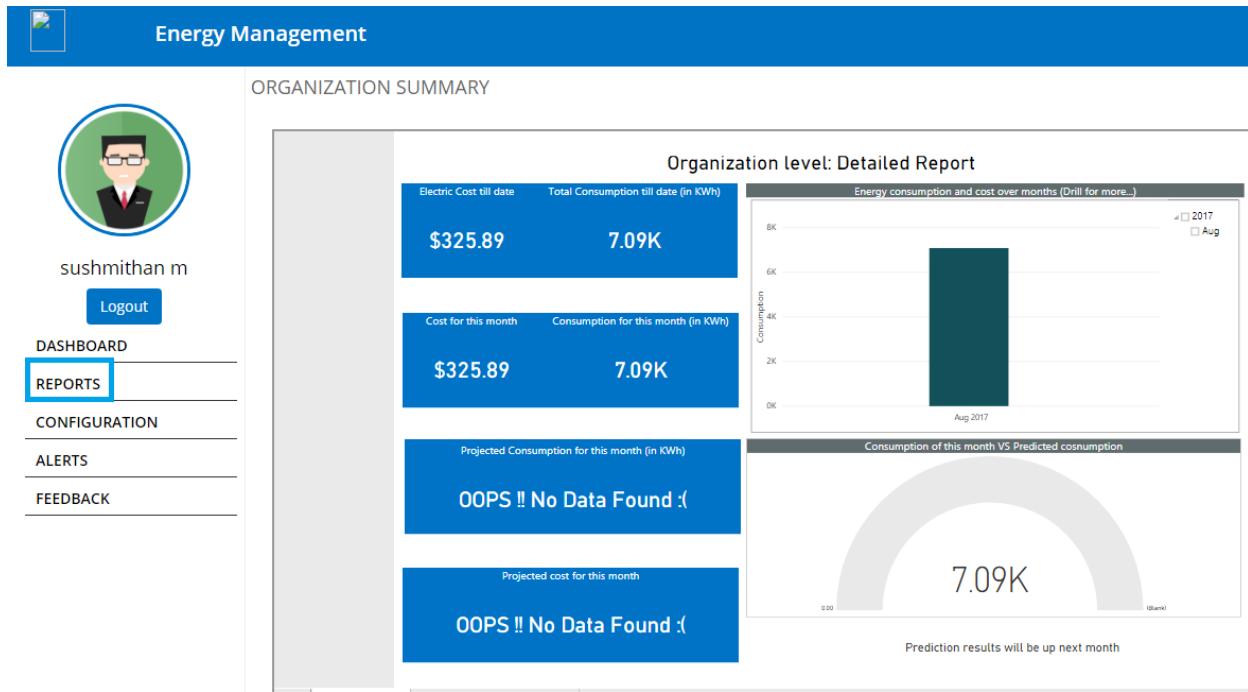
Enter them in the respective tabs (summary reports in the first column, detailed report in the second column), then click on **Add**.

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

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**.

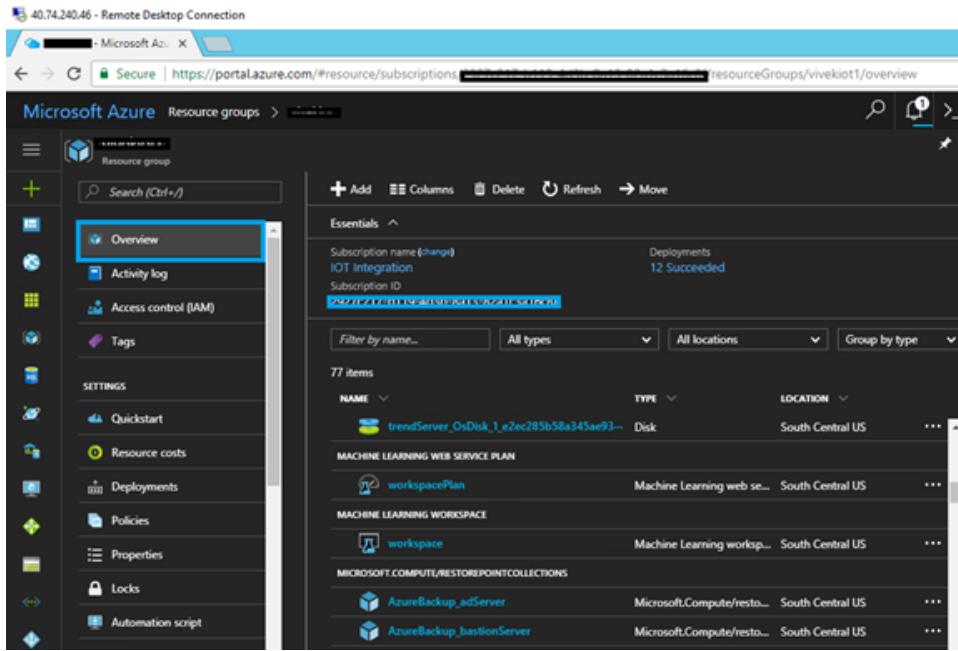
The screenshot shows the Energy Management application interface. On the left, there is a sidebar with a user profile picture of a man with glasses, the name "sushmithan m", a "Logout" button, and a navigation menu with options: DASHBOARD, REPORTS, CONFIGURATION (which is highlighted with a blue border), and FEEDBACK. The main content area has a header "Premise Configuration", "Premise-Building Mapping", and "PI Server Configuration". Below these, under "Power BI Credentials", three fields are shown: a client ID field containing "4722d592-4fac-41f3-91c1-04e17238ca40", a client secret field containing "bQRulQQUhrZMKWHeLwsjeVTFj/zOOAty6rAdKbUtTl8=", and two other fields whose values are redacted with blue bars. A blue "Add" button is located at the bottom right of this section.

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



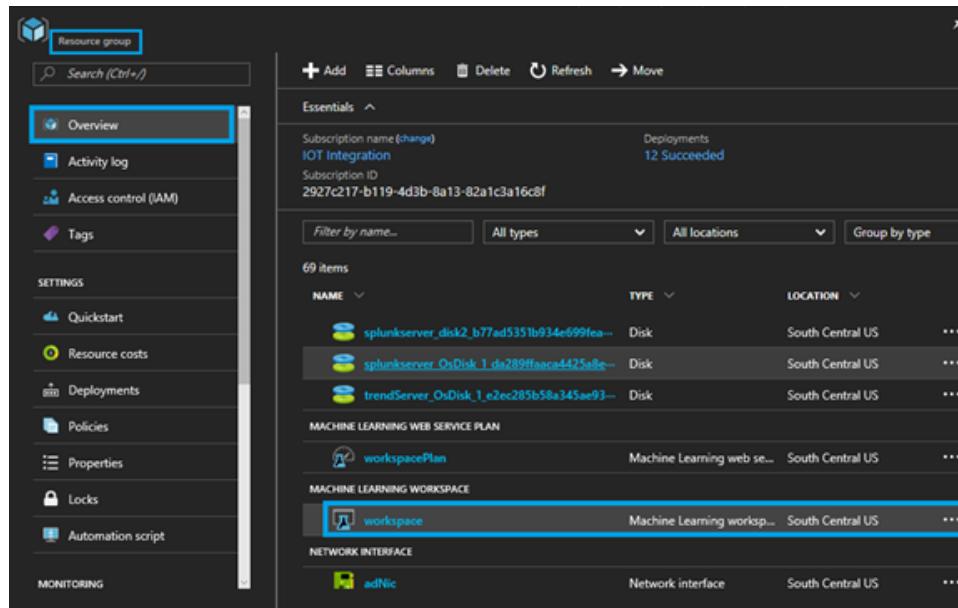
12. Machine Learning Experiment

1. Login into the Bastion host and open the Azure portal in it. Navigate to the Resource Group



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**.



NAME	TYPE	LOCATION
splunkserver_disk2_b77ad5351b934e699fea...	Disk	South Central US
splunkserver_OsDisk_1_d289ffac4425a8e...	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
adNic	Network interface	South Central US

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

The screenshot shows the 'Overview' tab selected in the left sidebar of the Azure Machine Learning workspace. The main content area displays the 'Essentials' section with the following details:

		Type
Resource group	(change)	PaidStandard
Status	Enabled	Storage
Location	South Central US	mistrjv556
Subscription name	(change)	
IOT Integration		
Subscription ID	2927c217-b119-4d3b-8a13-82a1c3a16c8f	

Below this, there is a section titled 'Additional Links' containing three items:

- Launch Machine Learning Studio** (highlighted with a blue box)
- Launch Machine Learning Gallery**
- Launch Machine Learning Web Service Management**

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

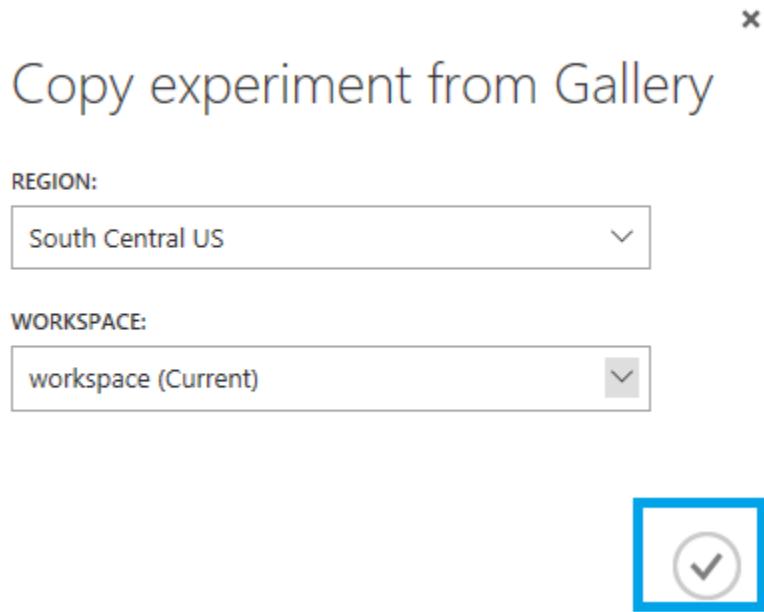
The screenshot shows the Microsoft Azure Machine Learning Studio login page at studio.azureml.net. The page features a 'Welcome to Azure Machine Learning' header and a 'Try it for free' section. It includes a video thumbnail for a 'Quick Tour of Azure ML'. On the right, there is a 'Sign In' button and links for 'Not an Azure ML user?' and 'Sign up here'. At the bottom, there is a 'Pricing & FAQ' link.

5. Copy the below url and open it in new browser and click on **Open in Studio**, this will launch the Experiment to the **workspace**.

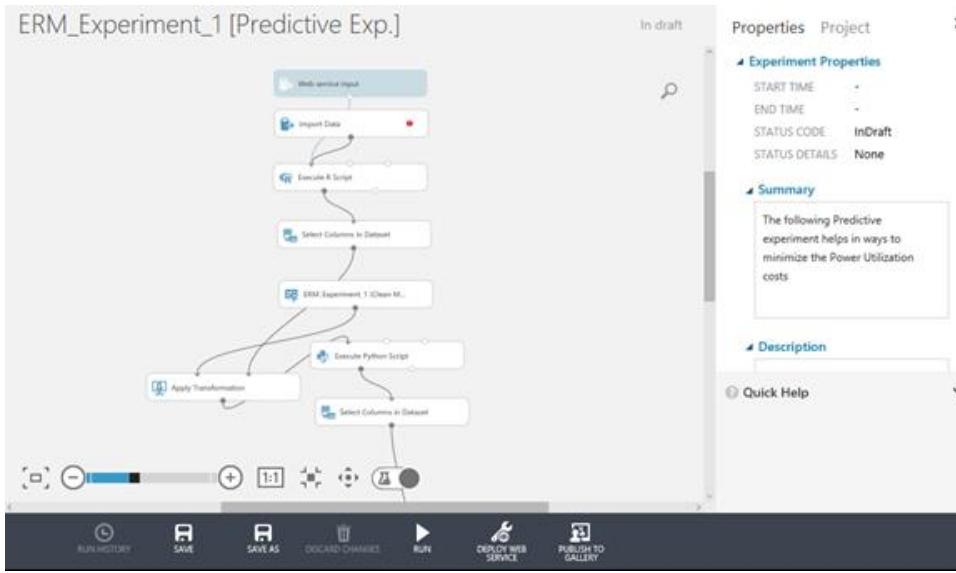
Path : <https://gallery.cortanaintelligence.com/Experiment/ERM-Experiment-1-Predictive-Exp>

The screenshot shows a web browser window with the address bar displaying 'gallery.cortanaintelligence.com/Experiment/ERM_Experiment_1/Predictive-Exp'. The page title is 'Cortana Intelligence Gallery'. Below the title, there's a navigation bar with links for 'Browse all', 'Industries', 'Solutions', 'Experiments', 'Machine Learning APIs', 'Custom Modules', 'Learning', and 'More'. The main content area is titled 'EXPERIMENT' and shows 'ERM_Experiment_1 [Predictive Exp.]'. It includes a profile picture of 'Mohammed Khan', a date 'August 4, 2017', and a message 'Be the first to like.' There are sections for 'Summary' and 'Description'. A preview image of the experiment flow is shown on the right, along with a 'Open in Studio' button and an 'Add to Collection' link.

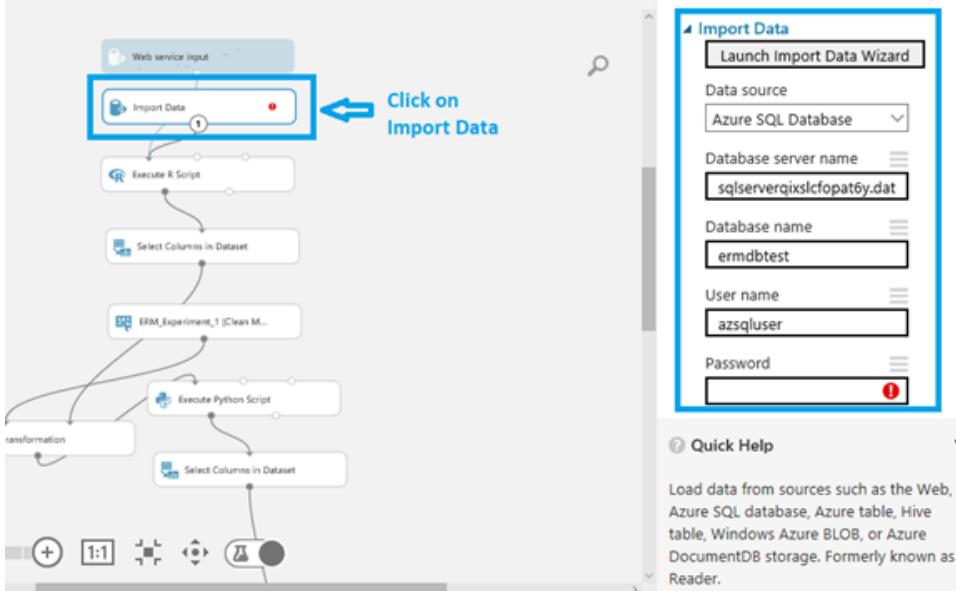
6. The below screen will appear in the new tab, click on the **tick mark**.



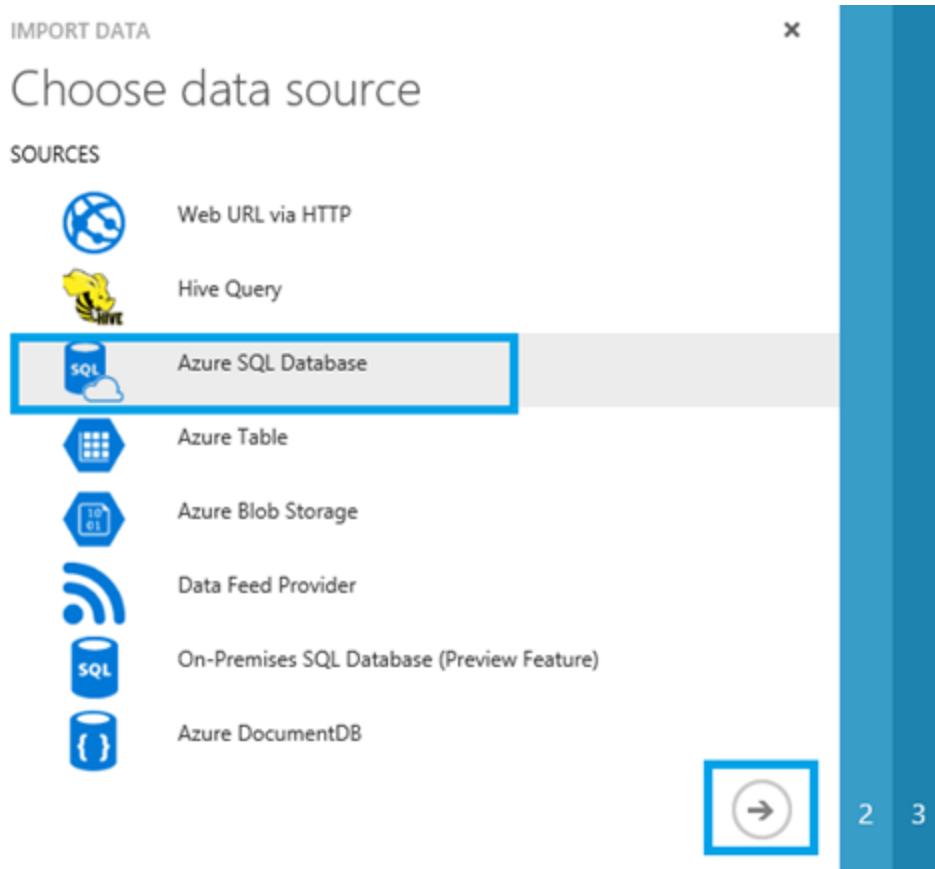
7. The experiment gets downloaded in our workspace.



- Once the experiment got pulled in the workspace, click on **Import Data**. Now click on **Launch Import Data Wizard** from right side menu.



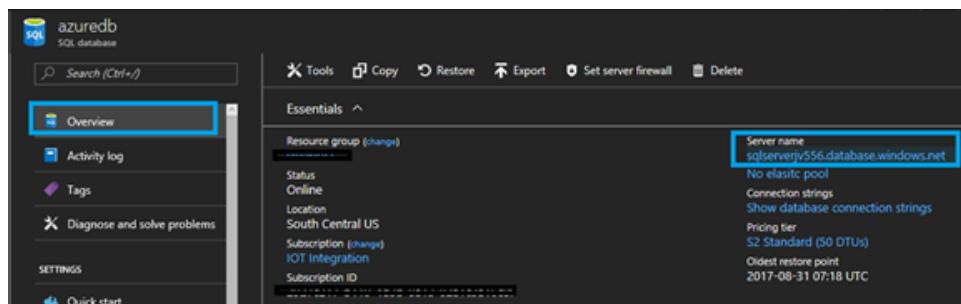
- Select **Azure SQL Database** and click on Next icon “->”.



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** and click on **Test connection**.

Click on Next icon.

IMPORT DATA

Connect to Azure SQL Database

Subscription ID

Enter values manually...

Database server name

sqlserverjv556.database.windows.net

Database name

azuredb

User name

sqluser

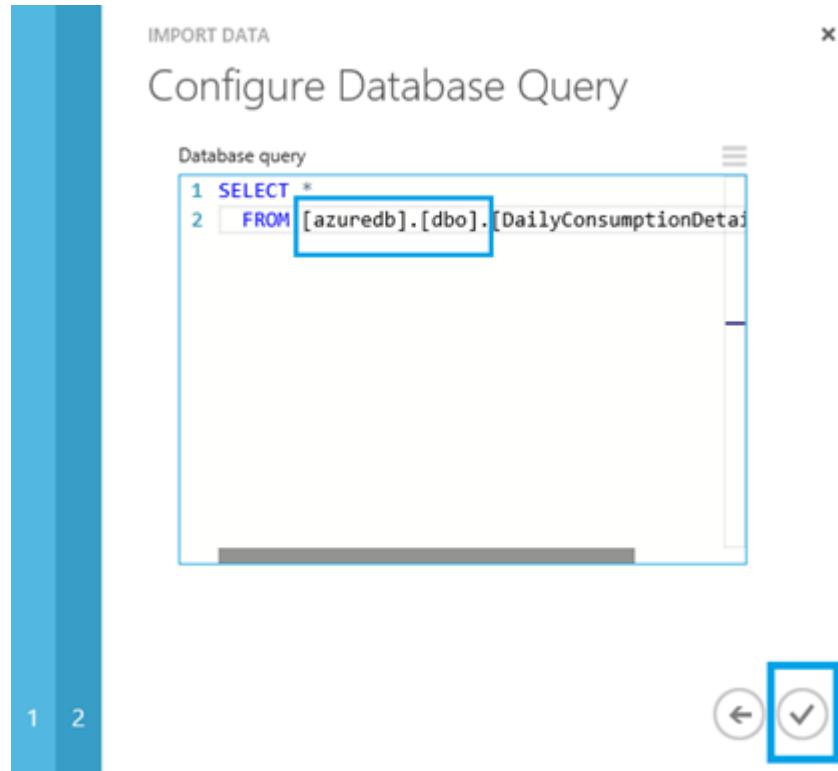
Password

Accept any server certificate (insecure)

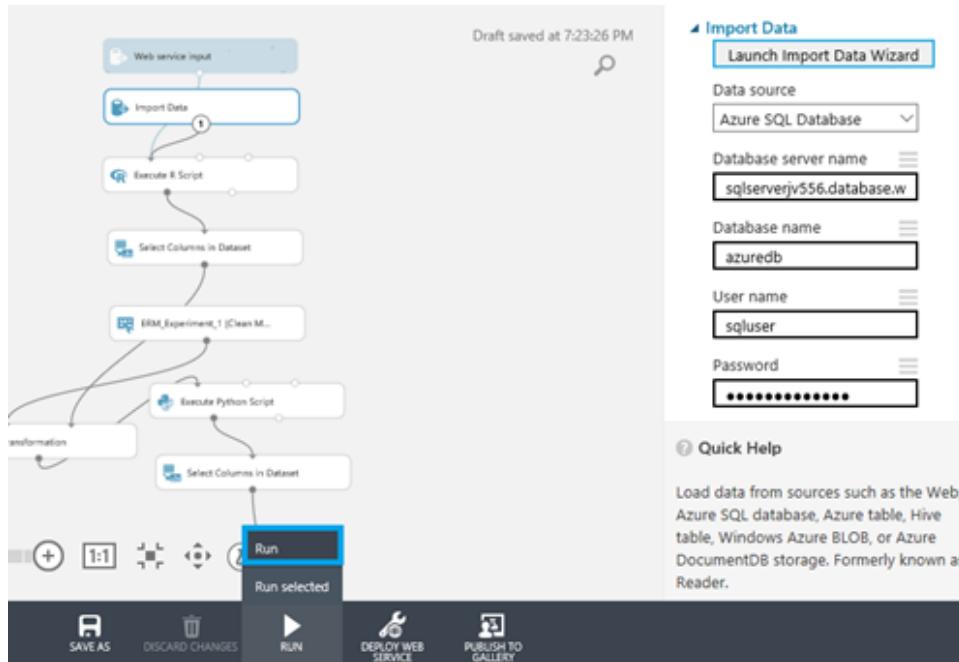
Test Connection

Test connection succeeded.

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



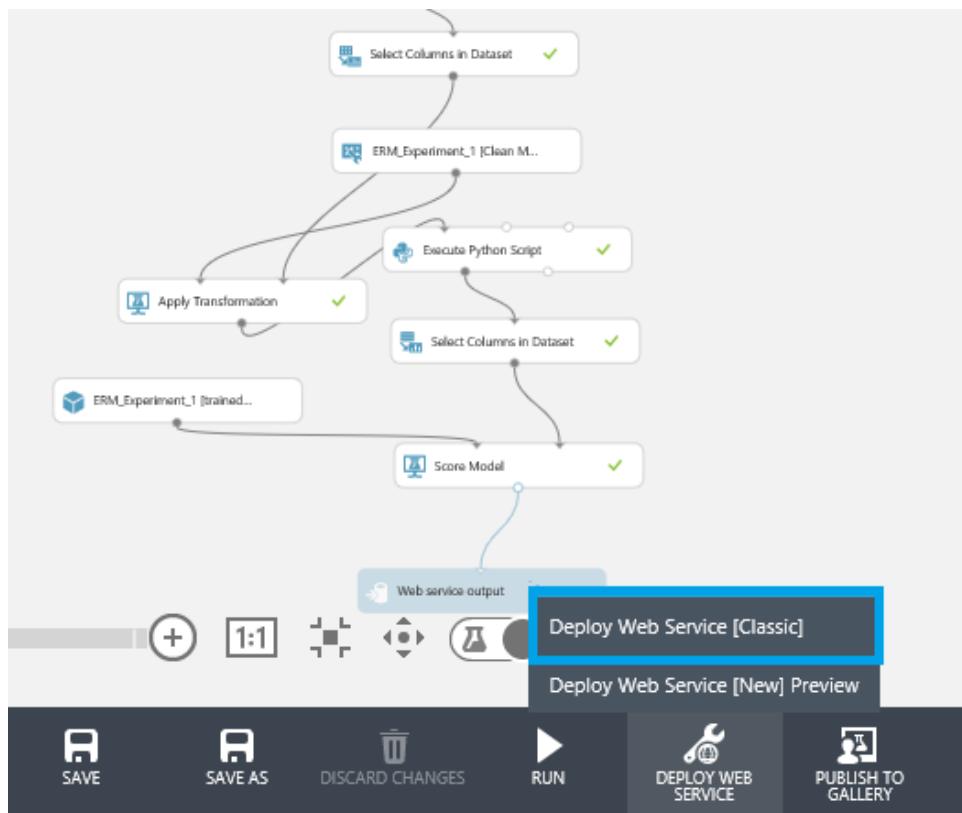
14. Once done run the experiment by right clicking on **Run** from bottom of the below screen and from the appeared menu click on **Run**.



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.



- Once the experiment gets deployed, the below screen will appear. Copy the **API Key** and save it for later use.

Click on Request/Response button under **API HELP PAGE** to get the **POST URL**.

erm_experiment_1 [predictive exp.]

DASHBOARD CONFIGURATION

General [New Web Services Experience](#) preview

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

Description
No description provided for this web service.

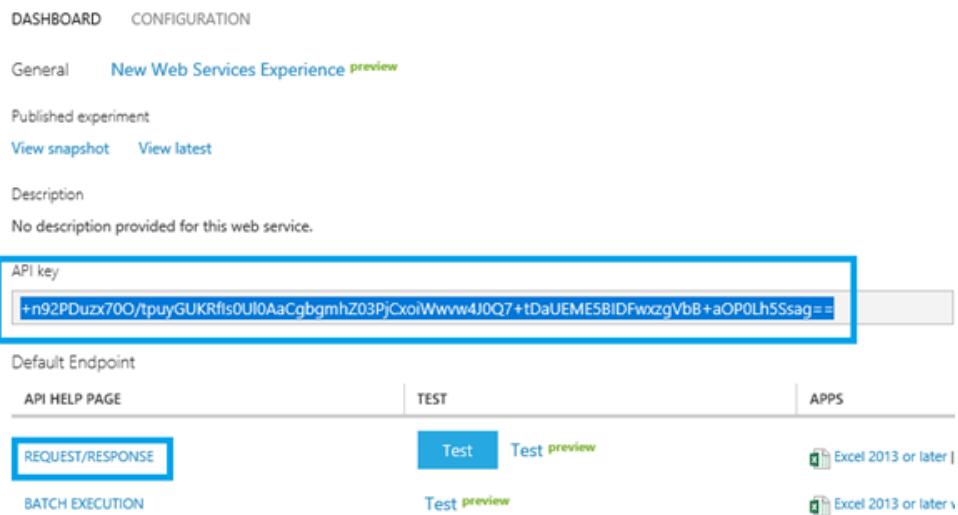
API key
`+n92PDuzx7O0/tputyGUKRfls0Ul0AaCgbgmhZ03PjCxoiWwww4J0Q7+tDaUEME5B1DFwxzgVbB+aOP0Lh5Ssag==`

Default Endpoint

API HELP PAGE TEST APPS

REQUEST/RESPONSE Test preview 

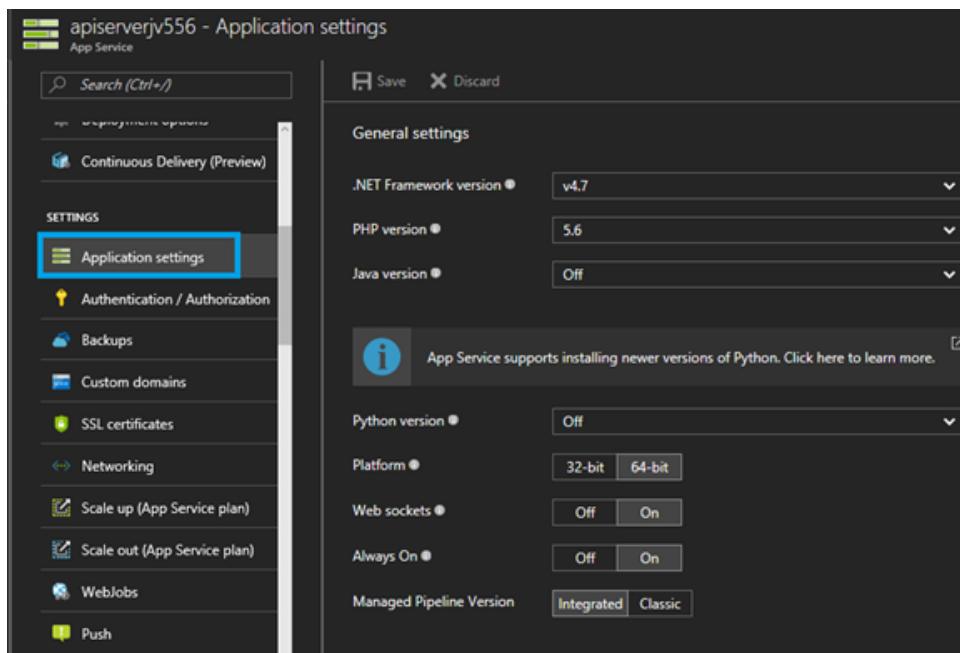
BATCH EXECUTION Test preview 



18. Copy the POST URL and save it for later use.

v

19. Navigate to **Application settings** of **apiserver** webapp and scroll down to **App Settings**.



20. Add

AzureMIAnomalyDetectionApiKey with apikey value from **step 29**.

AzureMIAnomalyDetectionApiUrl with Post URL from **step 30**.

SETTINGS	
Application settings	b2cSignInPolicyId: B2C_1_sinpolicy2
Authentication / Authorization	b2cClientSecret: 39iOK5g0lJN\$rl7
Backups	b2cChangePasswordPolicy: B2C_1_cpasspolicy
Custom domains	EmailHost: iothost
SSL certificates	EmailHostPort: 25
Networking	EmailSender: noreply@gmail.com
Scale up (App Service plan)	EmailHostPassword: Password@1234
Scale out (App Service plan)	BlobStorageConnectionString: DefaultEndpointsProtocol=https;AccountName=webjo...
Webjobs	AzureMIAnomalyDetectionApiKey: +n92PDuzx700/tputyGUKRfis0U0AaCgbgmhZ03PjCxi...
Push	AzureMIAnomalyDetectionApiUrl: https://ussouthcentral.services.azureml.net/workspaces/...

21. Restart the **apiserver**.

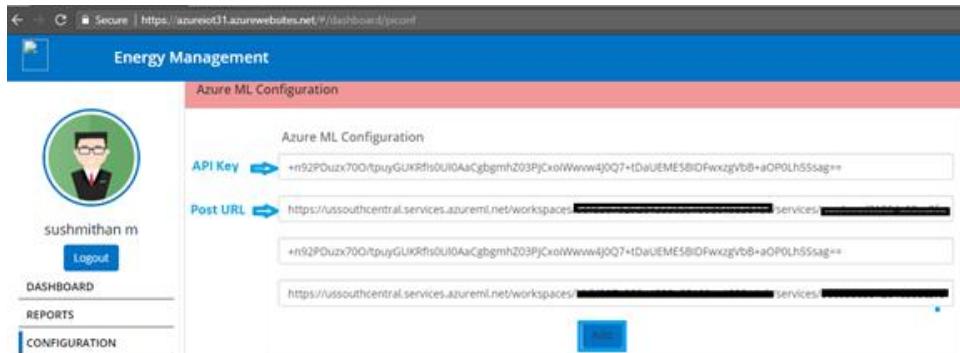
SETTINGS	
Application settings	
Authentication / Authorization	b2cSignInPolicyId B2C_1_sinpolicy2
Backups	b2cClientSecret 39iOK5g0LjN\$rfi7
Custom domains	b2cChangePasswordPolicy B2C_1_cpasspolicy
SSL certificates	EmailHost iothost
Networking	EmailHostPort 25
Scale up (App Service plan)	EmailSender noreply@gmail.com
Scale out (App Service plan)	EmailHostPassword Password@1234
WebJobs	BlobStorageConnectionString DefaultEndpointsProtocol=https;AccountName=webjo...
	AzureMIAnomalyDetectionApiKey +n92PDuzx700/tputyGUKRfls0Uf0AaCgbgmhZ03PjCxol...
	AzureMIAnomalyDetectionApiUrl https://ussouthcentral.services.azureml.net/workspaces/...

22. Login to the web application.

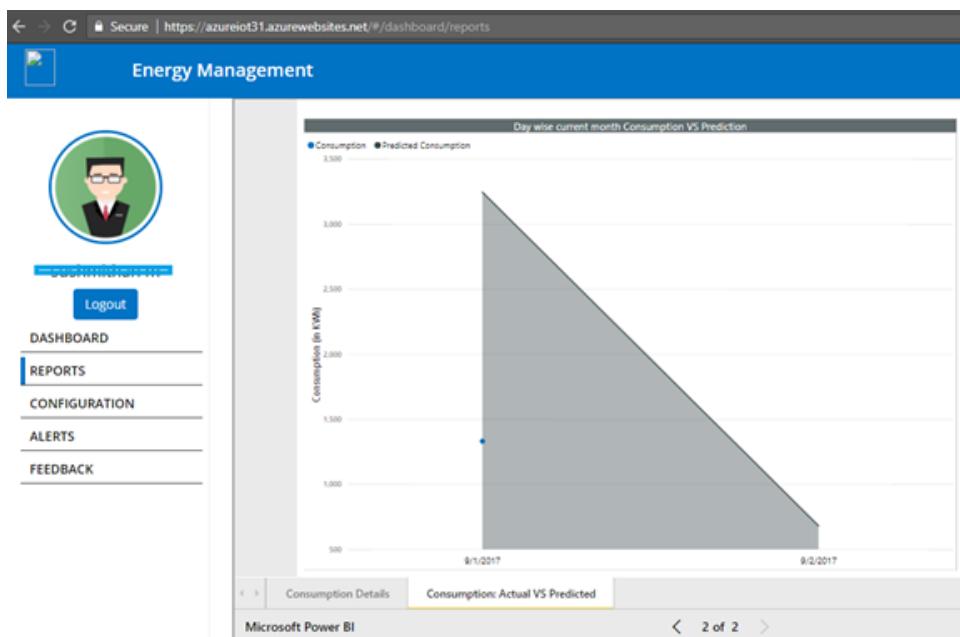


23. Navigate to **Azure ML Configuration** and add the **API Key** and **POST URL**.

Click on **Add**.

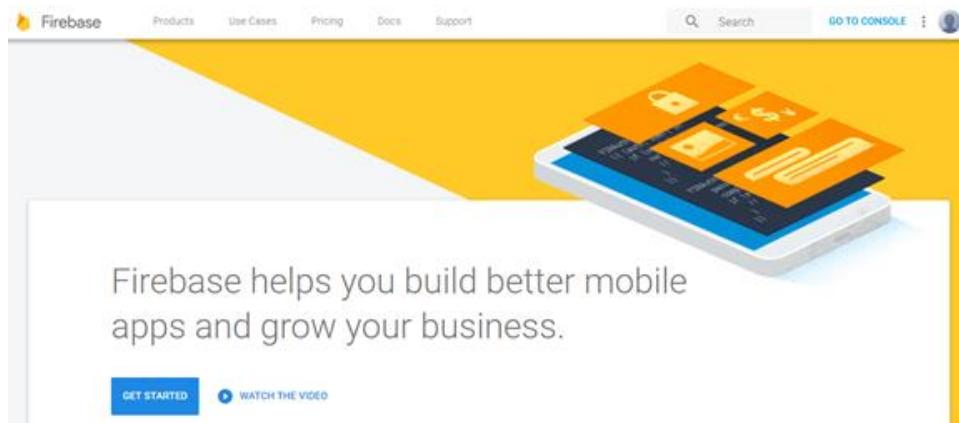


24. Click on **REPORTS** and click on **Consumption: Actual VS Predicted** of the bottom of the screen to view the Actual Vs Predicted graph.

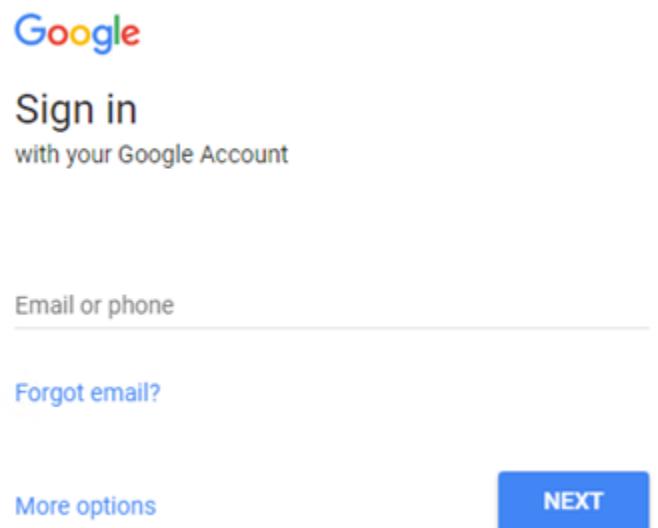


13. Firebase Configuration

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**.



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 ?
iotproject-7fb4a Edit

Country/region ?

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 MESSAGING**.

Save the **Server key** and **Legacy Server Key**.

Create a project

Project name

Project ID [Edit](#)

Country/region

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](#)

The screenshot shows the Firebase console interface. On the left, there's a sidebar with navigation links like Overview, Analytics, Database, Storage, Hosting, Functions, Test Lab, Crash Reporting, and Performance. The main area is titled 'Settings' and has tabs for GENERAL, CLOUD MESSAGING, ANALYTICS, ACCOUNT LINKING, and SERVICE ACCOUNTS. Under the GENERAL tab, there's a section for 'Project credentials' with a table. The first row in the table is highlighted with a blue border and contains the 'Server key' column which shows a long string of characters.

Key	Token
Server key	AAAA_...vVZSM...R059QwFSHvkspndz7L...vvMm6OPkL...z2Ef2ov68lQjvIzUfc6AbshxEZre...kITzTaK...Nj6ICTZzPuSR...kApCMwYc...5m10g@uZU...ydr...eG4B...n7us...KE
Legacy server key	AizallyOnQ...7Exdal...J...P...Pie...GK...MeMpg...U
Sender ID	1096497325347

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

The screenshot shows the 'Cloud Messaging' tab selected in the Firebase console. Under 'Project credentials', there is a table with two rows. The first row contains 'Server key' and its value, which is a long string of characters starting with 'AAAA_0vvZSM...'. The second row contains 'Legacy server key' and its value, which is 'AlzaSyAbTdFA76Xo5THJRqIdRWLfd...'. A blue box highlights the 'Server key' row.

Key	Token
Server key	AAAA_0vvZSM... alITzTakN_Nj6iCTzPwRJbka... 1096497325347
Legacy server key	AlzaSyAbTdFA76Xo5THJRqIdRWLfd... 1096497325347

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

The dialog box has a title 'Add Firebase to your web app' and a close button 'X'. It contains a text area with instructions: 'Copy and paste the snippet below at the bottom of your HTML, before other script tags.' Below this is a code snippet:

```

<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
// Initialize Firebase
var config = {
  apiKey: "AlzaSyAbTdFA76Xo5THJRqIdRWLfd...",
  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>

```

A blue box highlights the configuration object in the code. To the right of the code is a 'COPY' button. At the bottom, there are links: 'Get Started with Firebase for Web Apps', 'Firebase Web SDK API Reference', and 'Firebase Web Samples'.

```

<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
// Initialize Firebase
var config = {
  apiKey: "AlzaSyAbTdFA76Xo5THJRqIdRWLfd...",
  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>

```

8. Open postman

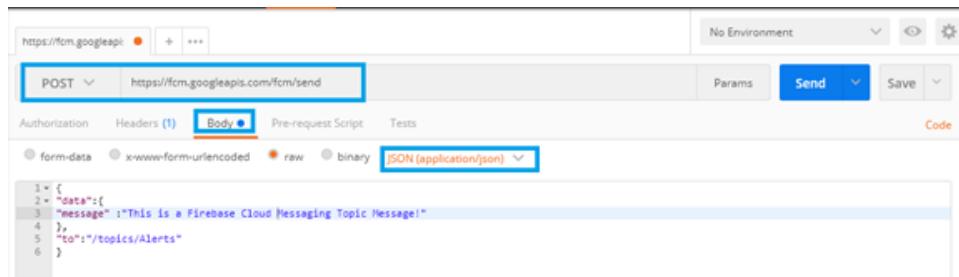
- Change the Params to **POST** and paste the below URL

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

- Click on Body and enter the content

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

- Select the text to **Json**



9. Click on **Headers**, Add a new key called **Authorization** and give the value as **key=<Legacy Server Key>** which was obtained during step5. Click on **Send**.

The screenshot shows a Postman request to `https://fcm.googleapis.com/fcm/send`. The Headers tab is selected, containing two entries: `Content-Type: application/json` and `Authorization: key=AlzaSyDnQxhxI7Sxdalc0jPBP9e_GKKSMeMpgiU`. The Body tab shows a JSON response with a single key-value pair: `{"message_id": "6201689062246313932"}`. The status bar at the bottom indicates `200 OK` and `Time: 1108 ms`.

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

Note: For Messaging Receiver Id give **/topics/Alerts**

The screenshot shows the **Firebase Configuration** page in the Webapp. On the left is a sidebar with a user profile picture, a **Logout** button, and navigation links: **DASHBOARD**, **REPORTS**, **CONFIGURATION** (which is selected), **ALERTS**, and **FEEDBACK**. The main area has a red header bar labeled **Firebase Configuration**. Below it are several input fields:
 - Legacy Server Key: AlzaSyDnQxhxI7Sxdalc0jPBP9e_GKKSMeMpgiU
 - Project ID: iotproject-7fb4a.firebaseio.com
 - Storage Bucket: https://iotproject-7fb4a.firebaseio.com
 - Topic Path: /topics/Alerts

A blue button at the bottom right says **Updated Firebase Configuration**. A green button below it says **Configuration Updated**.

