

## Contents

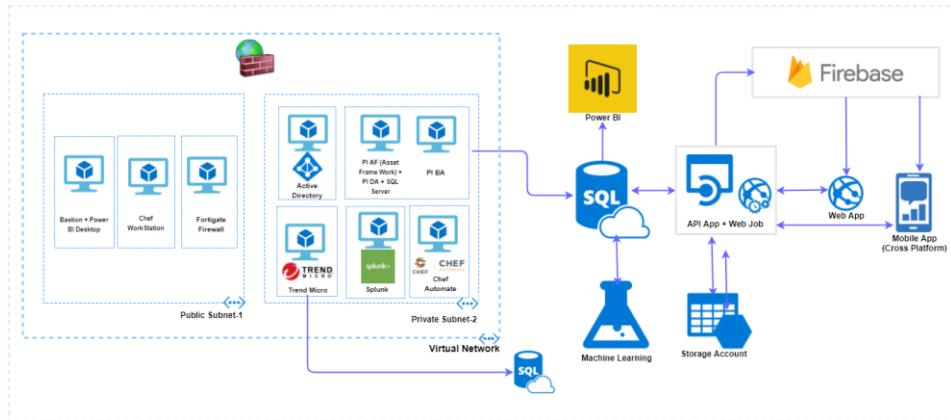
1. Architecture.....	3
1.1. Data Flow Architecture Diagram.....	3
2. High Level Deployment Process to be Followed .....	4
3. Deployment Costs .....	5
4. Prerequisites.....	7
4.1. Azure B2C Tenant Creation and Configuration.....	7
4.2. Power BI Configuration.....	27
4.3. Dynatrace Account Creation (If 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

Commented [UD1]: Trend and splunk documentation has to added

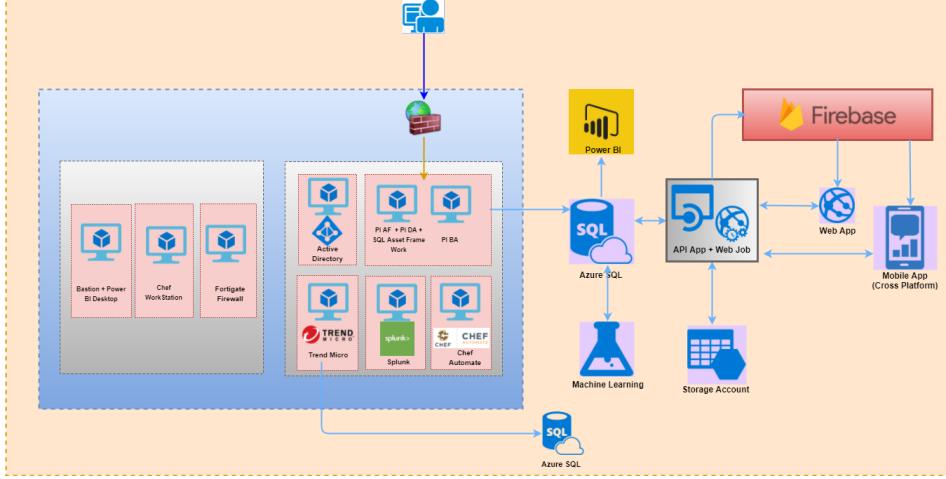
Commented [KO2RI]: Chef,splunk,trend added

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

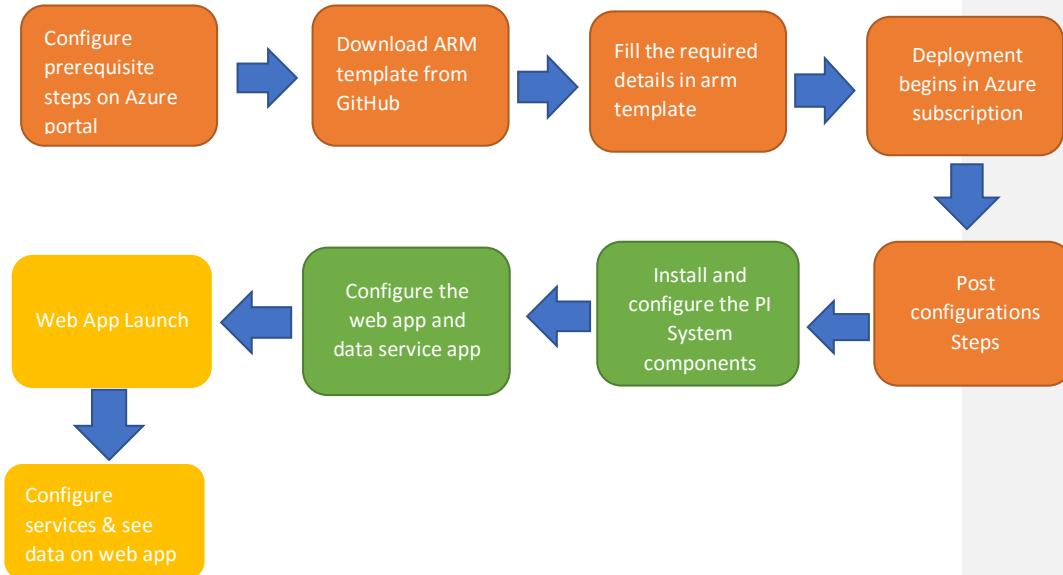
## 1. Architecture

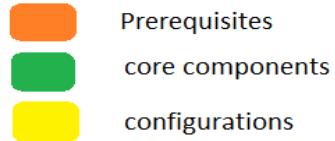


### 1.1. Data Flow Architecture Diagram



## 2. High Level Deployment Process to be Followed





### 3. Deployment Costs

**Commented [UD3]:** Add small section before to show all the full forms like what is PIAFSQL Server etc

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

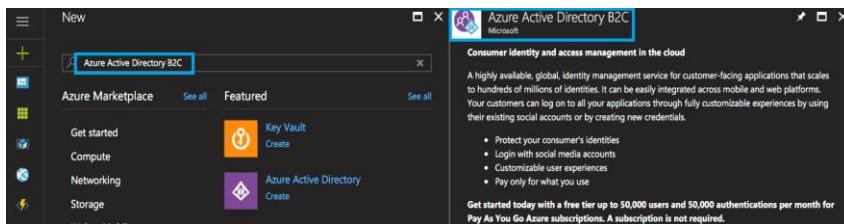
1. The Azure AD B2C Tenant should be created and register your web application.
2. Create an account in Power BI.
3. Dynatrace account creation in SAAS.

### 4.1. Azure B2C Tenant Creation and Configuration

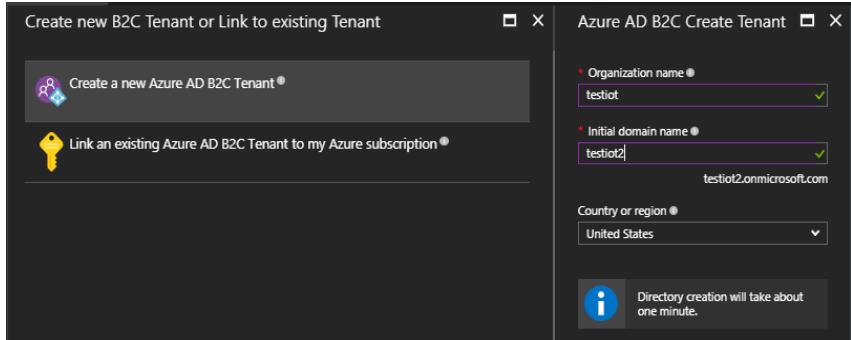
Creating Azure AD B2C tenant is a one-time activity, if you have a B2C Tenant already created by your admin then you should be added into that tenant as Global Administrator to register your app to get the B2C tenant id, application id and sign-in/sign-up policies.

#### Follow Below steps to create Azure AD B2C Tenant:

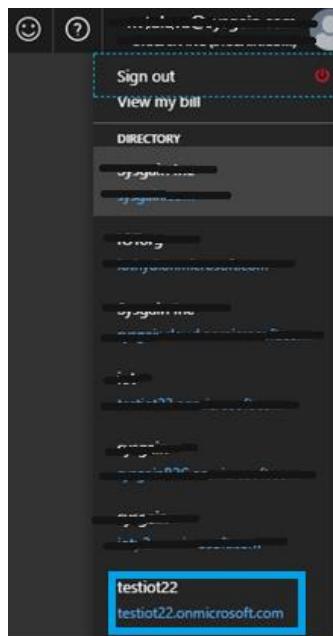
1. Create a new B2C tenant in **Azure Active Directory B2C**. You'll be shown a page with the information on Azure Active Directory B2C. Click **Create** at the bottom to start configuring your new Azure Active Directory B2C tenant.



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.

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

- 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.

**Commented [AS4]:** Before 6<sup>th</sup> point add a point as  
In your B2C tenant click on more services in bottom right  
corner and search for Azure AD B2C to access your B2C you  
created.

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

Search (Ctrl+F)

+ Add    Upload Policy

Overview

MANAGE

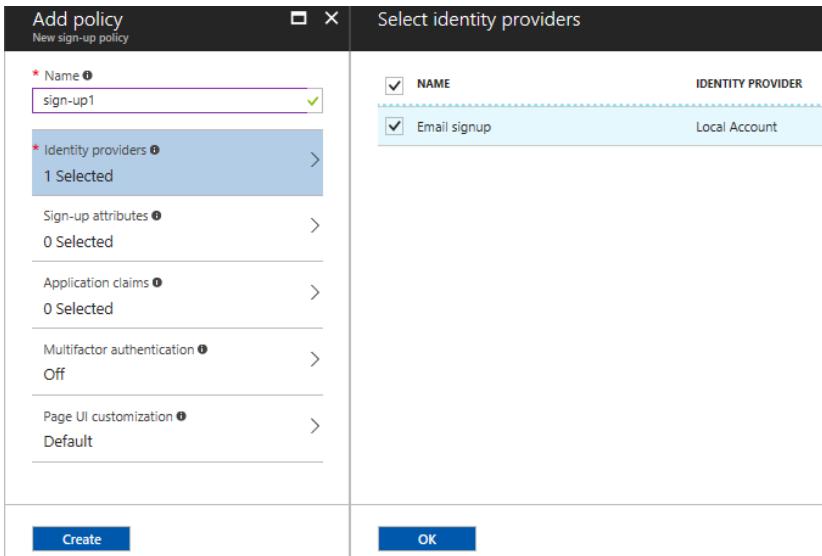
- Applications
- Identity providers
- User attributes
- Users and groups

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

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

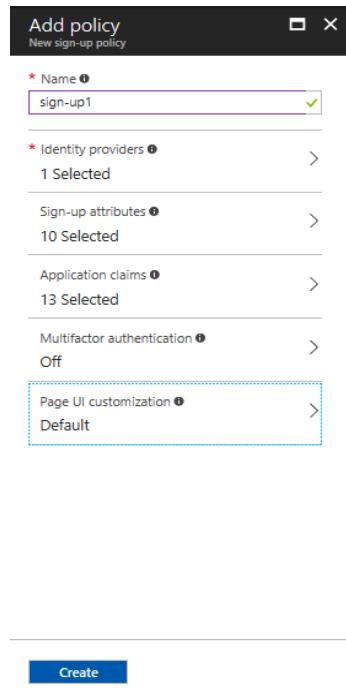


8. Select all the **Sign-up attributes** as show below.

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

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

**Commented [AS5]:** Add a point and screenshot for Application claims as you kept for Sign-up attributes



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 contains navigation links for Overview, Applications, Identity providers, User attributes, Users and groups, Sign-up or sign-in policies, Profile editing policies, Password reset policies, Sign-up policies (which is selected and highlighted in blue), Sign-in policies, and All policies. The main area displays a search bar and a list of policies. One policy is listed: "B2C\_1\_sign-up1" (Default template).

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 page. On the left, there's a sidebar with links for Overview, Applications, Identity providers, User attributes, Users and groups, and various policy types. Under Policies, 'Sign-in policies' is highlighted with a blue background. At the top right, there are 'Add' and 'Upload Policy' buttons. The main area has a search bar and a message saying 'No policies found'.

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

The screenshot shows two overlapping dialog boxes. The left box is 'Add policy' with a title 'New sign-in policy'. It has a 'Name' field containing 'sign-in1', an 'Identity providers' section showing '0 Selected', and other sections for Application claims, Multifactor authentication, and Page UI customization. A 'Create' button is at the bottom. The right box is 'Select identity providers' with a table:

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

An 'OK' button is at the bottom of this box.

**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 include NAME, CLAIM TYPE, DATA TYPE, DESCRIPTION, and ATTRIBUTE TYPE. The claims are: City, Country/Region, Display Name, Email Addresses, Given Name, Identity Provider, Job Title, Postal Code, State/Province, Street Address, Surname, and User's Object ID. At the bottom left is a 'Create' button, and at the bottom right is an 'OK' button.

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

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

The screenshot shows the 'Add policy' dialog box. The 'Application claims' section is highlighted with a blue dashed box. The '12 Selected' count is also highlighted with a blue dashed box. At the bottom left is a 'Create' button.

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

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

Search (Ctrl+ /) + 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-in1  
Default template

16. Click on **Profile editing policies**

Azure AD B2C - Profile editing policies  
adiotp2.onmicrosoft.com

Search (Ctrl+ /) + Add Upload Policy

Overview

MANAGE

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

POLICIES

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

No policies found

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

The screenshot shows the 'Add policy' dialog with the title 'Select identity providers'. On the left, under 'Identity providers', 'Local Account Signin' is selected. On the right, a table lists 'NAME' and 'IDENTITY PROVIDER' with 'Local Account Signin' checked. At the bottom are 'Create' and 'OK' buttons.

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

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

The screenshot shows the 'Add policy' dialog with the title 'Select profile attributes'. Under 'Profile attributes', all options are selected. On the right, a table lists various profile attributes like City, Country/Region, Display Name, etc., each with a checked checkbox. At the bottom are 'Create' and 'OK' buttons.

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

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

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

**Create**      **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 dark header "Azure AD B2C - Profile editing policies" and a sub-header "adiotp2.onmicrosoft.com". It includes a search bar "Search (Ctrl+/" and navigation links for "Overview", "MANAGE" (Applications, Identity providers, User attributes, Users and groups), and "POLICIES" (Sign-up or sign-in policies, **Profile editing policies**, Password reset policies, Sign-up policies). The "Profile editing policies" link is highlighted with a blue background. The main content area has a search bar "Search" and a list entry "B2C\_1\_profile-edit1 Default template". A "Add" button with a plus icon and an "Upload Policy" button with a file icon are located at the top of the main content area.

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

Azure AD B2C - Password reset policies  
adotp2.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

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

Add policy X

New password reset policy

\* Name \*  
password-change1 ✓

\* Identity providers \*  
0 Selected

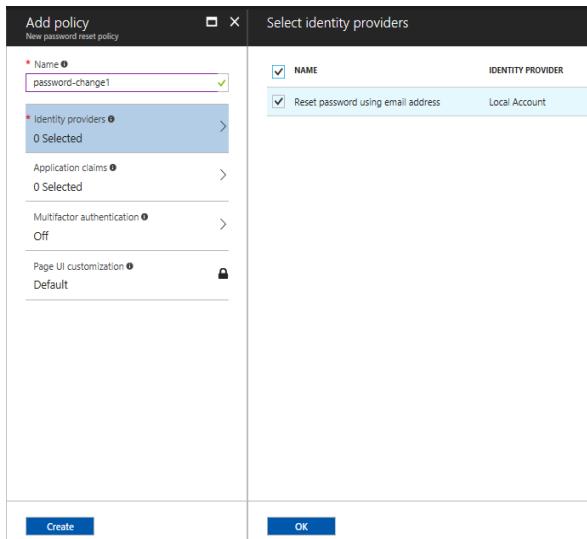
Application claims \*  
0 Selected

Multifactor authentication \*  
Off

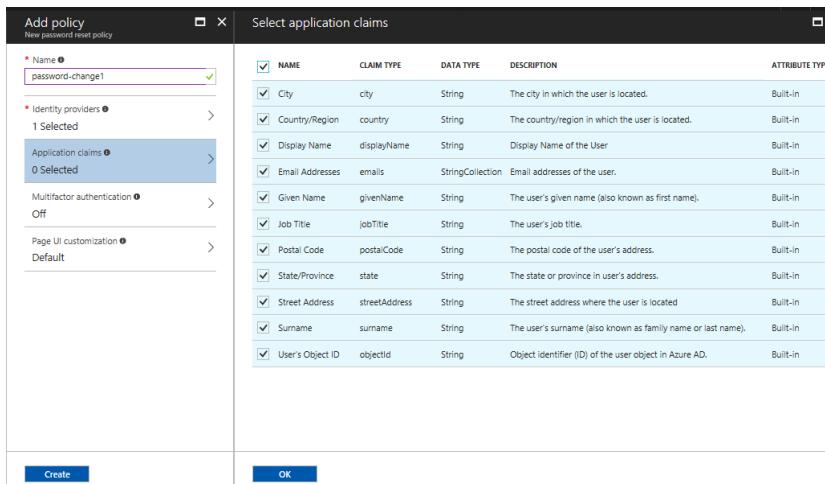
Page UI customization \*  
Default 🔒

**Create**

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



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



26. Click on **Create**.

Add policy X

New password reset policy

\* Name i  
password-change1 ✓

---

\* Identity providers i >  
1 Selected

Application claims i >  
11 Selected

Multifactor authentication i >  
Off

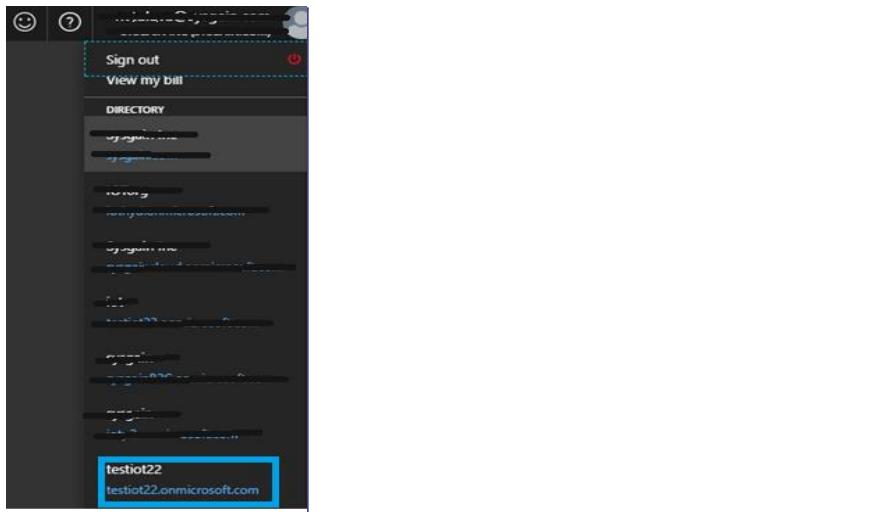
Page UI customization i >  
Default

Create

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

The screenshot shows the Azure AD B2C - Password reset policies interface. The left sidebar contains navigation links for Overview, Applications, Identity providers, User attributes, Users and groups, Sign-up or sign-in policies, Profile editing policies, Password reset policies (which is selected and highlighted in blue), Sign-up policies, Sign-in policies, and All policies. The main content area features a search bar at the top with the placeholder "Search (Ctrl+Shift+F)" and a "Upload Policy" button. Below the search bar, a list displays a single item: "B2C\_1\_password-change1" with the sub-label "Default template".

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



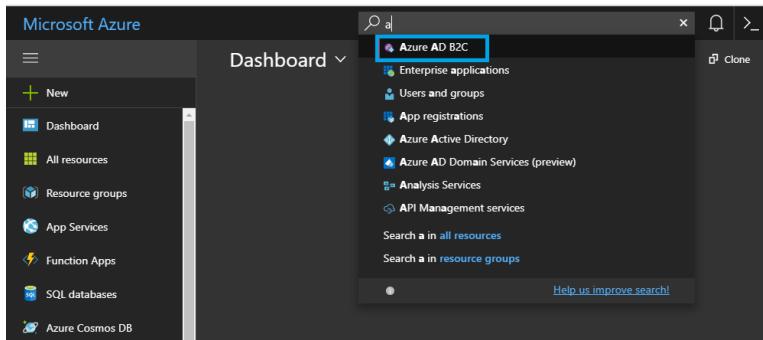
Commented [UD6]: Is this the correct image???

Commented [OM7R6]: Yes.after we create the tenant we see like this.

Commented [UD8R6]: The tenant is already created on point 3... do you still need this here?

Commented [KO9R6]: Point 3 shows the created tenant in one account ,this one showing after link existing tenant to my azure subscription in another account

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

Azure AD B2C - Applications  
testio22.onmicrosoft.com

+ Add

NAME	APPLICATION ID
contoso	0696fb08-2cfa-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:

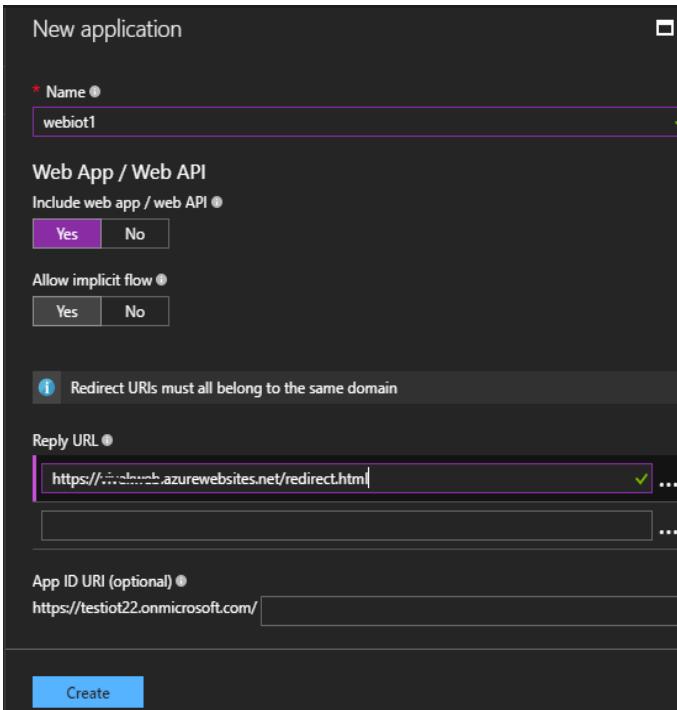
**https://<name of the web app>.azurewebsites.net/redirect.html**

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.

**Commented [AS10]:** Reply URL section according to below screenshot.

**Commented [UD11]:** Pls mention at the end to hit "Create" button

**Commented [KO12R11]:** updated

Azure AD B2C - Applications  
testiot22.onmicrosoft.com

**Search (Ctrl+ /)**

**Overview**

**MANAGE**

- Applications
- Identity providers
- User attributes

**+ Add**

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

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

webiot1 - Keys

**Search (Ctrl+ /)**

**GENERAL**

- Properties
- Keys**

**+ Generate key**

**App key ●**

26X\*\*\*\*\*

**Save** **Discard**

34. **Copy** the secret key.

webiot1 - Keys

**Search (Ctrl+ /)**

**GENERAL**

- Properties
- Keys**

**Save** **Discard** **+ Generate key**

**App key ●**

26X\*\*\*\*\*

%%\$88MxGK\$Sv6Ofz

## 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	Report and Dashboard APIs	Other APIs
<input checked="" type="checkbox"/> Read All Datasets	<input checked="" type="checkbox"/> Read All Dashboards	<input checked="" type="checkbox"/> Read All Groups
<input checked="" type="checkbox"/> Read and Write All Datasets	<input checked="" type="checkbox"/> Read All Reports	<input checked="" type="checkbox"/> Create Content
	<input checked="" type="checkbox"/> Read and Write All Reports	

### 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 PERMIS...	DELEGATED PERMIS...
Power BI Service (Microsoft.Azure.AnalysisServices)	0	5
Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)	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**.

**Commented [AS13]:** Mention click on Save after this step.  
**Commented [KO14R13]:** updated

Permission	Requires Admin
Access the directory as the signed-in user	No
Read directory data	Yes
Read and write directory data	Yes
Read and write all groups	Yes
Read all groups	Yes
Read all users' full profiles	Yes
Read all users' basic profiles	No
Sign in and read user profile	No

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

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

**Required permissions**

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

**Enable Access**

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

No application permissions available.

**DELEGATED PERMISSIONS**

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

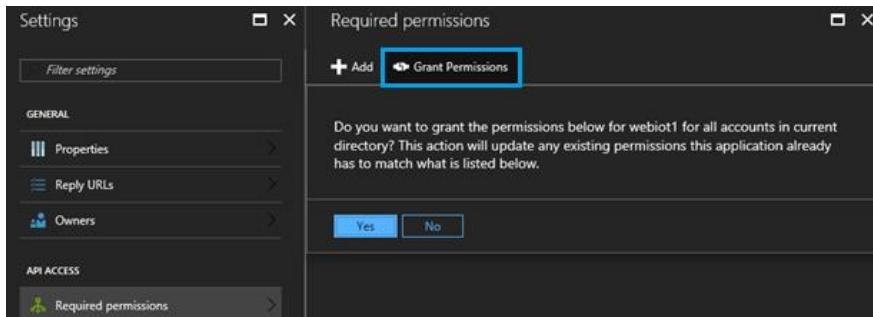
6. The user can see the number of permissions which have been added.

**Settings**

**Required permissions**

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

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



#### 4.3. 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".

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

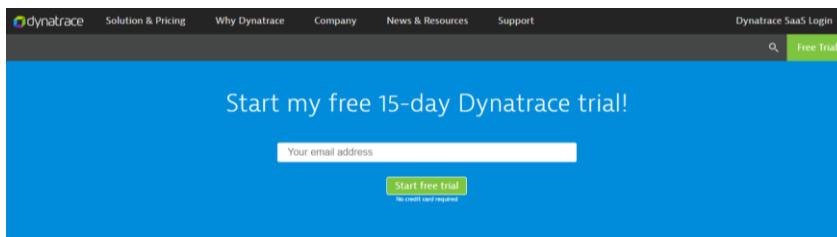
**New Users:** Please follow the below steps for "Sign up to Dynatrace trial SaaS for 15 days."

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

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

- 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!



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

The screenshot shows the "Account details" step of the Dynatrace account creation process. The page has a dark background. At the top, there are three tabs: "Create account" (disabled), "Account details" (highlighted in blue), and "Select your region". Below the tabs, the heading "Provide your account details" is centered. There are several input fields: "First name" (with a placeholder "L"), "Last name" (empty), "Company" (empty), "Country" (a dropdown menu), "Phone number" (with a placeholder "Optional"), and "Partner or promo code" (with a placeholder "Optional"). At the bottom of the form, there is a checkbox labeled "Tell me more about application performance." and a small explanatory text.

- Select your region and click on “Create account”.

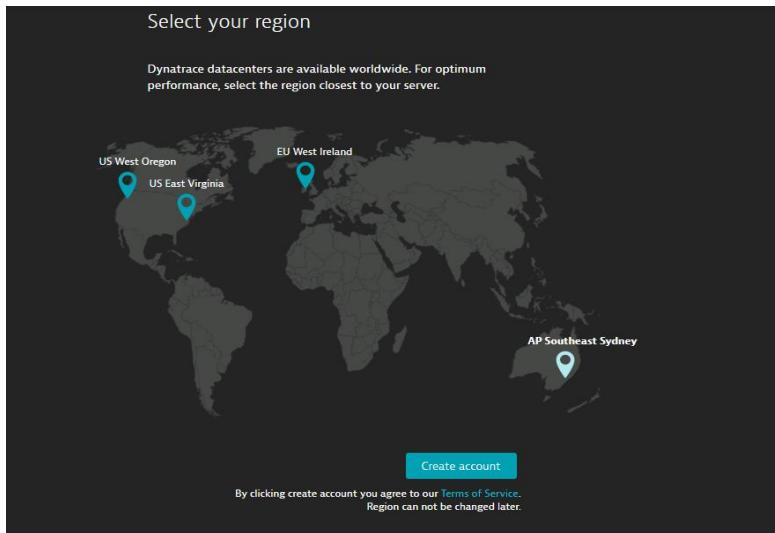
**Commented [UD15]:** Pls also mention..what to do when you already have an account

**Commented [KO16R15]:** Updated

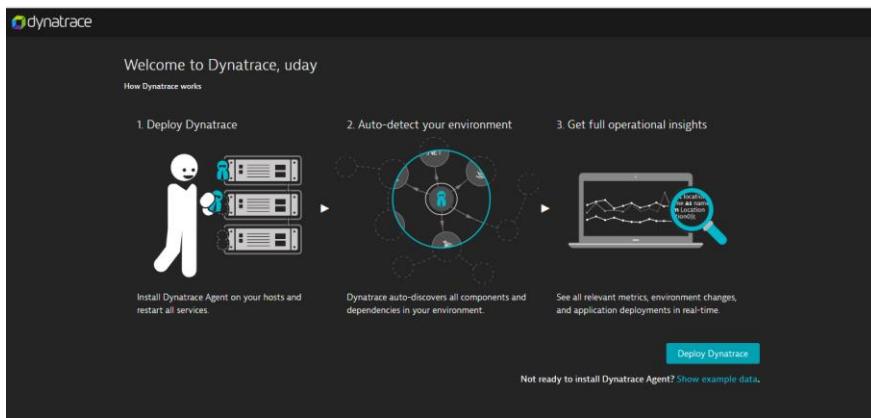
**Commented [UD17R15]:**

**Commented [AS18]:** Mention following link  
[https://www.dynatrace.com/trial/?vehicle\\_name=https://www.dynatrace.com/](https://www.dynatrace.com/trial/?vehicle_name=https://www.dynatrace.com/)  
For free trial  
Or  
<https://www.dynatrace.com>

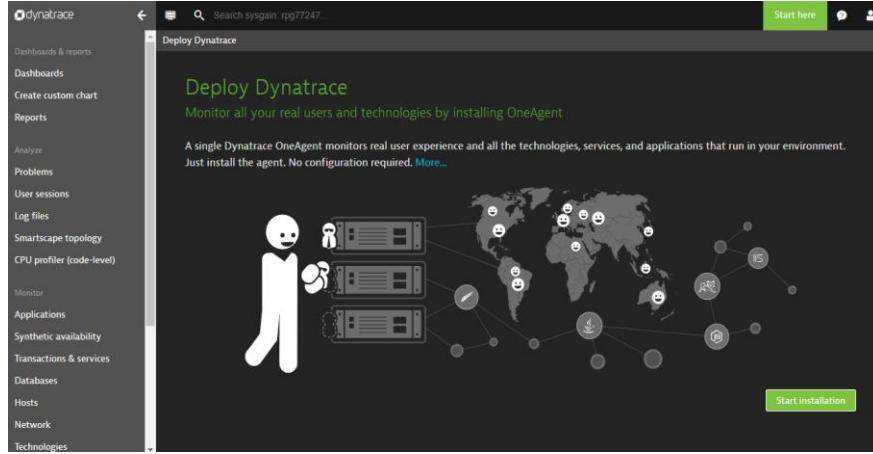
**Commented [KO19R18]:** updated



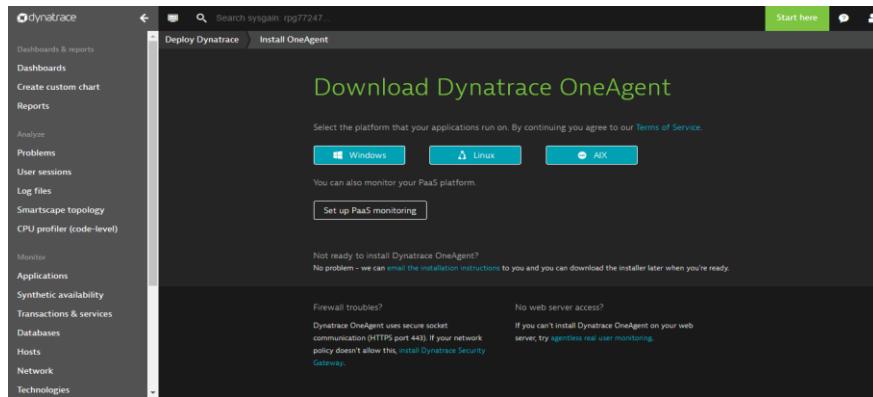
4. Click on "**Deploy Dynatrace**".



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

**Commented [UD20]:** Please check the input parameters are matching with template... I see new parameters added to template recently

**Commented [AS21]:** Update the metadata info from ARM template under description column.

Make sure you add metadata for all the parameters in the ARM template and same in documents, parameter table

**Commented [AS22]:** Add a an example in metadata of ARM template or a regular expression.

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 - <a href="https://azure.microsoft.com/en-us/pricing/details/app-service/">https://azure.microsoft.com/en-us/pricing/details/app-service/</a>	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_signuppolicy2)	
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)	

- Commented [UD23]: Do we need this in parameter??
- Commented [KO24R23]: Yes, user should give .
- Commented [AS25]: Add an example in metadata in arm template
- Commented [UD26]: Range of the ports??? Do we need this in parameter??
- Commented [KO27R26]: Its aDefault port number
- Commented [UD28R26]: Can the user enter any number here or just 25... if it is just 25 then I suggest move it to variables
- Commented [KO29R26]: 25 is required

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	

**Commented [AS30]:** Add a line in metadata saying refer the prereq section of deployment document for more info.. on all B2C related parameters. In Template

## 6. Azure Resource Manager Template Deployment

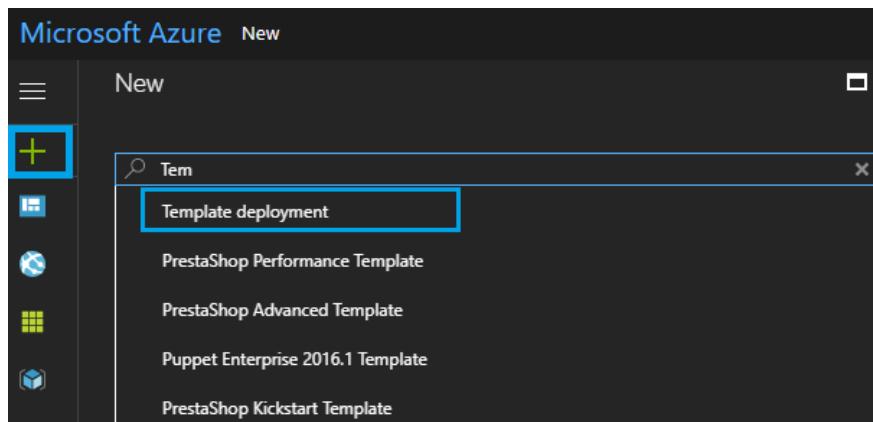
**Commented [UD31]:** On template make sure all parameters have tool tips

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 Azure Portal's 'Template deployment' blade. On the left, there's a sidebar with social sharing icons (Twitter, Facebook, LinkedIn, YouTube, Google+, Email) and sections for 'PUBLISHER' (Microsoft), 'LOGICAPP SUPPORTED' (none), and 'USEFUL LINKS' (Documentation). At the bottom of this sidebar is a large blue 'Create' button. The main content area is titled 'Custom deployment' with the subtitle 'Deploy from a custom template'. It includes a 'Learn about template deployment' section with links to 'Read the docs' and 'Build your own template in the editor' (which is also highlighted in blue). Below this are sections for 'Common templates' (with links to 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', and 'Create a SQL database') and 'Load a GitHub quickstart template' (with a search bar and a 'Type to start filtering...' placeholder). At the bottom right of the main content area are 'Pin to dashboard' and 'Purchase' buttons.

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

The screenshot shows the 'Edit template' blade. At the top, it says 'Edit template' and 'Edit your Azure Resource Manager template'. Below that are buttons for '+ Add resource', 'Quickstart template', 'Load file', and 'Download'. On the left, there's a sidebar with 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main area contains a JSON code editor with the following content:

```

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

```

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

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

Admin Username ⓘ

Admin Password ⓘ

Domain Name ⓘ

Bastion VM Size ⓘ

Chef Workstation VM Size ⓘ

Fortigate VM Size ⓘ

Ad Server VM Size ⓘ

Trend VM Size ⓘ

Splunk VM Size ⓘ

Chef Automate VM Size ⓘ

PIAFDASQL Server VMSize ⓘ

PIBA Server VMSize ⓘ

Website Name

Sql Administrator Login ⓘ

**Commented [AS32]:** Add a screenshot with all the parameters it can be divided into multiple screenshots  
The admin username and admin password and domain name parameters missing from the screenshot

**Commented [KO33R32]:** updated

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](#); both 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

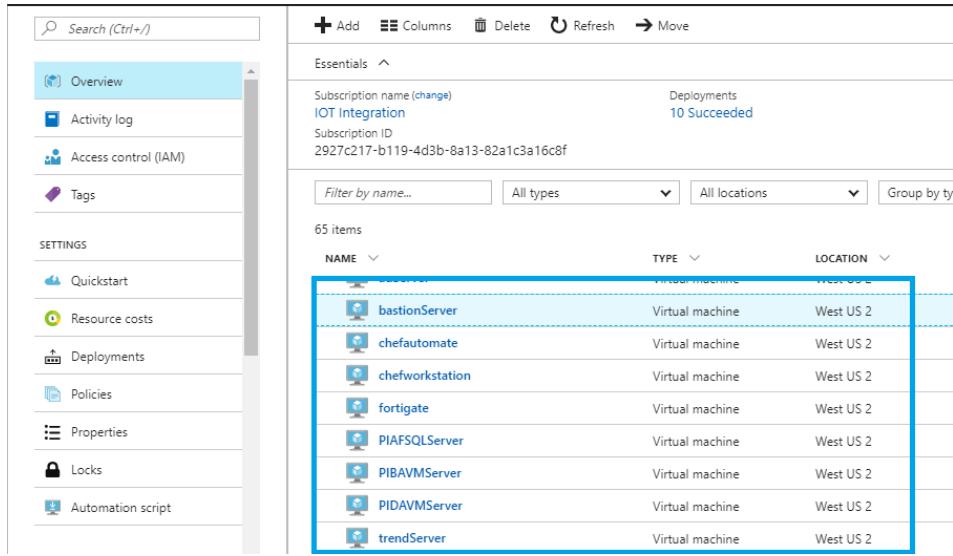
**Purchase**

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 various navigation options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, and Automation script. The main area is titled 'Essentials' and shows deployment details: Subscription name (IOT Integration), Deployments (10 Succeeded), and Subscription ID (2927c217-b119-4d3b-8a13-82a1c3a16c8f). A search bar at the top allows filtering by name, type, location, and group. The main table lists 65 items, specifically 8 virtual machines, ordered by Name. The columns are NAME, TYPE, and LOCATION. The virtual machines listed are: bastionServer, chefautomate, chefworkstation, fortigate, PIAFSQLServer, PIBAVMServer, PIDAVMServer, and trendServer. All are categorized as 'Virtual machine' and located in 'West US 2'. A blue rectangular box highlights the list of virtual machines.

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 (webjobStorageacctName)	Web job storage account
Website URL (websiteUrl)	We application URL

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

Outputs

ADMINUSERNAME	adminuser	
BASTIONFQDN	bastionserverstnh6.southindia.cloudapp.azure.com	
ADSERVERIPADDRESS	10.0.1.4	
PIAFSQLSERVERIPADDRESS	10.0.1.5	
PIBASERVERIPADDRESS	10.0.1.11	
WORKSTATIONFQDN	wsclientstnh6.southindia.cloudapp.azure.com	
CHEFAUTOMATEIPADDRESS	10.0.1.6	
CHEFAUTOMATELOGINUSERN...	adminuser	
TRENDIPADDRESS	10.0.1.10	
TRENDWEBUIUSERNAME	adminuser	
SPLUNKIPADDRESS	10.0.1.8	

SPLUNKWEBUIUSERNAME	admin	
FORTIGATEFQDN	fortigatestnh6	
AZURESQLENDPOINT	sqlserverstnh6.database.windows.net	
AZURESQLDBNAME	azuredb	
AZURESQLUSERNAME	sqluser	
WINDOWSSQLUSERNAME	sqluser	
WEBJOBSTRORAGEACCNTNAME	webjobstrstnh6	
WEBSITEURL	<a href="https://mshydapp.azurewebsites.net/">https://mshydapp.azurewebsites.net/</a>	

## 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.

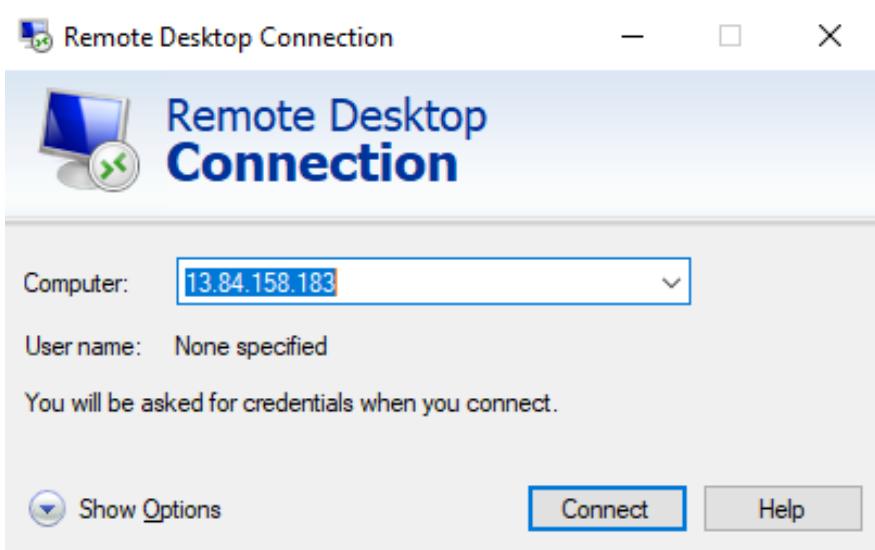
**Trend Micro Deep Security Manager (DSM):** This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents. The DSM is controlled using the web-based management console. Using the console, the administrator can define security policies, 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.

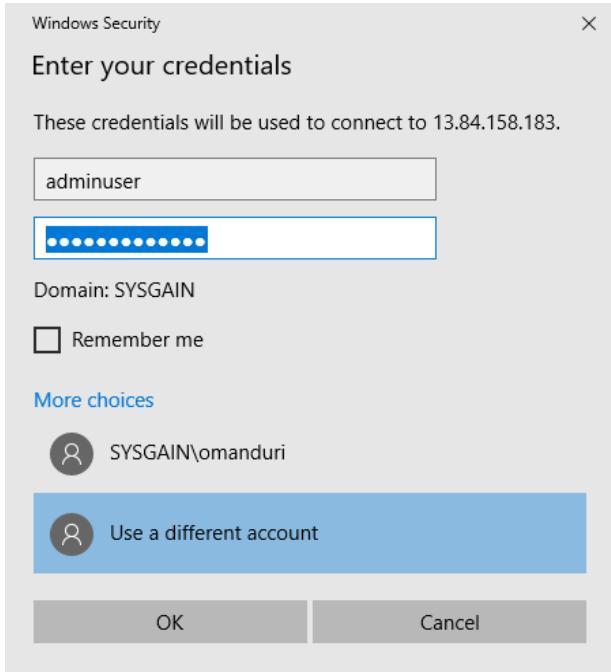
**Splunk Enterprise:** Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device.

### 7.1. Dynatrace

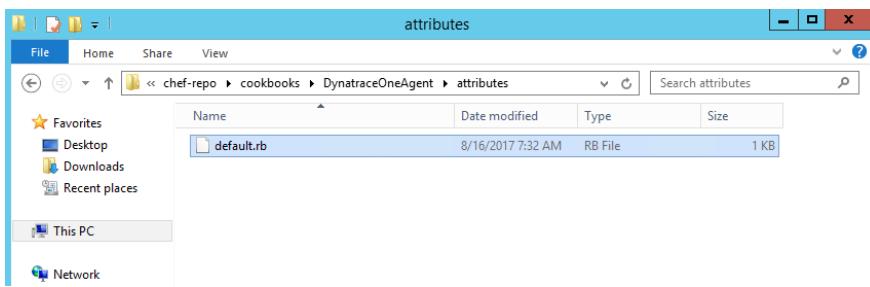
1. Log in to the **Chef Workstation** using the Public IP Address provided in the output section.



2. Enter the credentials provided in the output section.

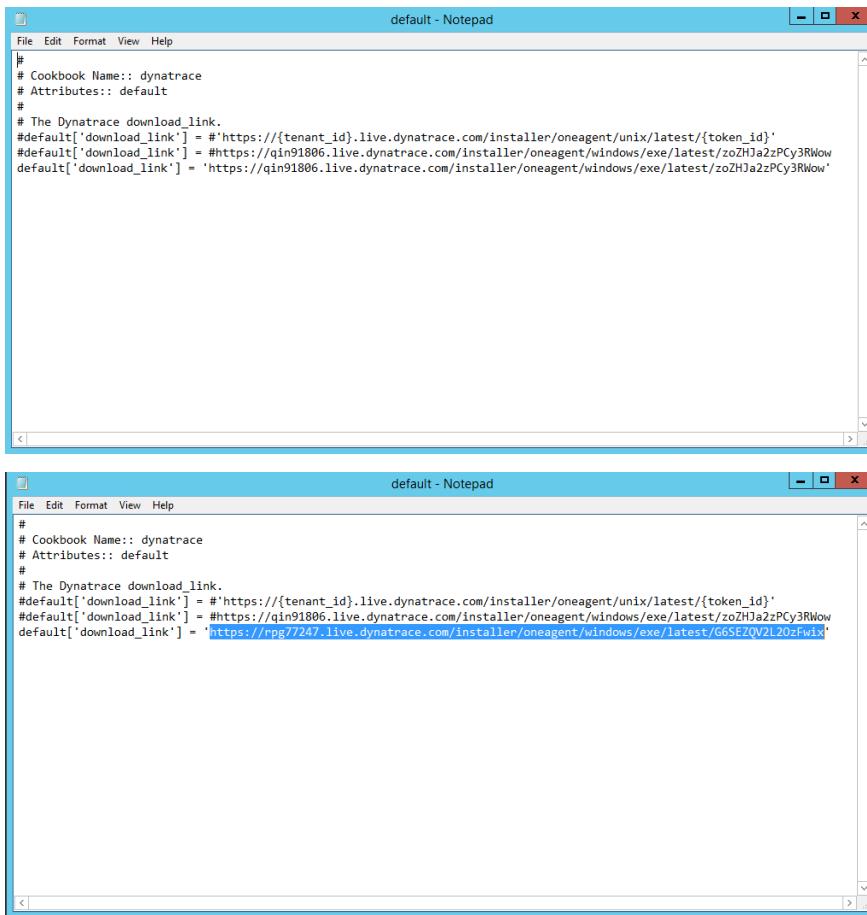


2. After logging in, navigate to **C:\Users\chef-repo\cookbooks\DynatraceOneAgent\attributes** and open the **default.rb** file.



3. Add the new unique url:

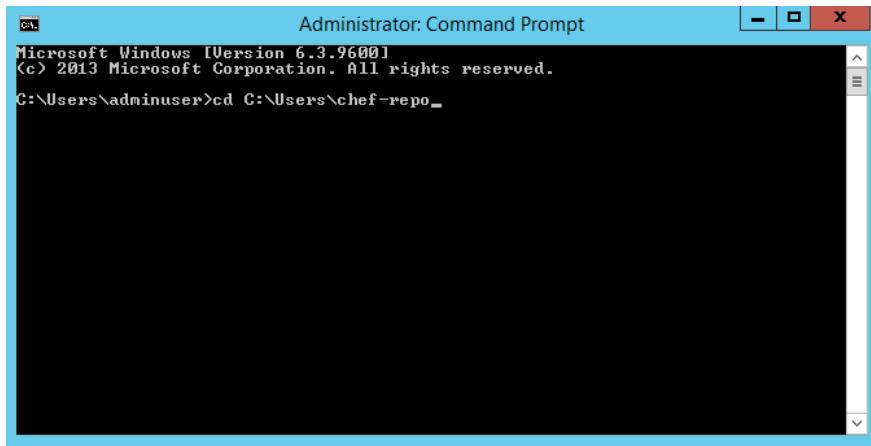
<https://rpg77247.live.dynatrace.com/installer/oneagent/windows/exe/latest/G6SEZQV2L2OzFwix> as the last link and **save** the file.



The image shows two side-by-side windows of Microsoft Notepad. Both windows have a title bar 'default - Notepad' and a menu bar 'File Edit Format View Help'. The content in both windows is identical, displaying a Ruby code snippet for a cookbook named 'dynatrace'. The code defines a variable 'download\_link' with three default values for different platforms: Unix, Windows, and a specific Fwix URL. The Fwix URL is highlighted in blue, indicating it is the new unique URL added in step 3.

```
# 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'
```

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



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

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

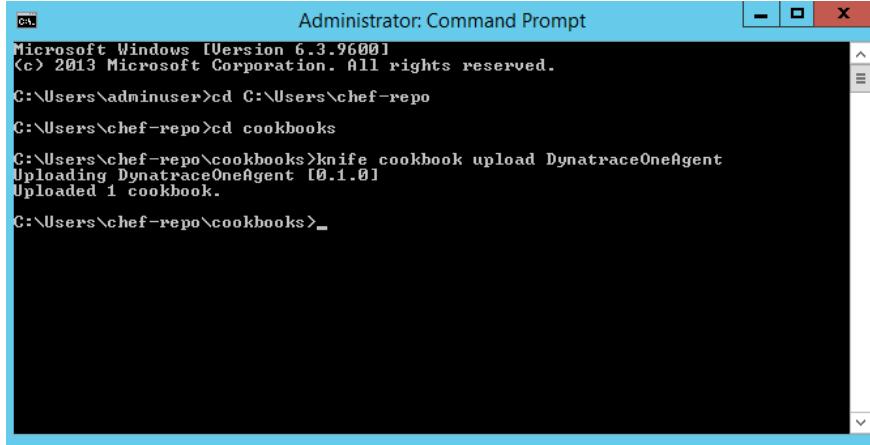
5. Change the directory to **cookbooks** and run the below command to upload the "DynatraceOneAgent":

```
knife cookbook upload DynatraceOneAgent
```



```
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
```



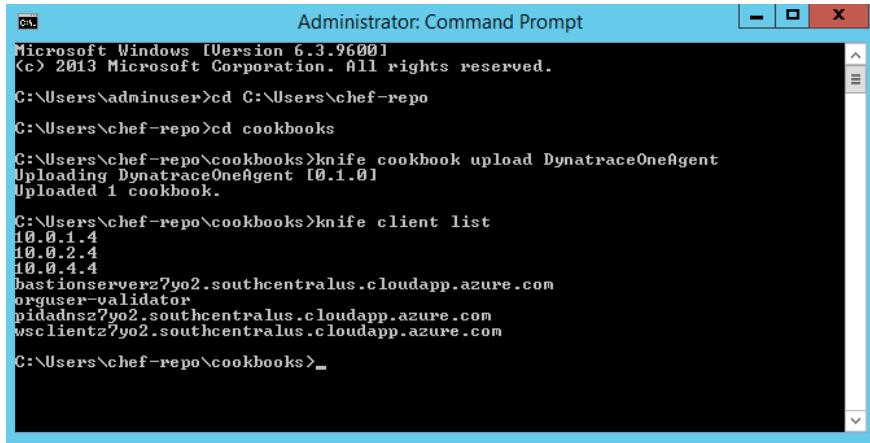
```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

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

```
knife client list
```



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

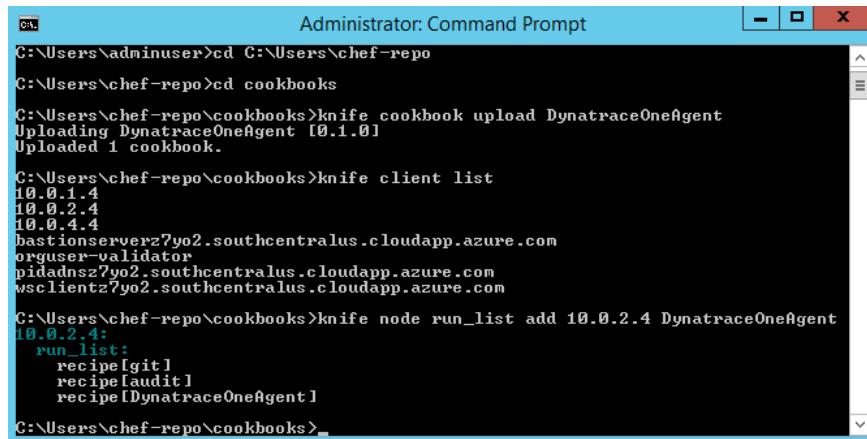
C:\Users\admininuser>cd C:\Users\chef-repo
C:\Users\chef-repo>cd cookbooks
C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserver2?yo2.southcentralus.cloudapp.azure.com
orguser-validator?
pidadnsz?yo2.southcentralus.cloudapp.azure.com
wsclientz?yo2.southcentralus.cloudapp.azure.com

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

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

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



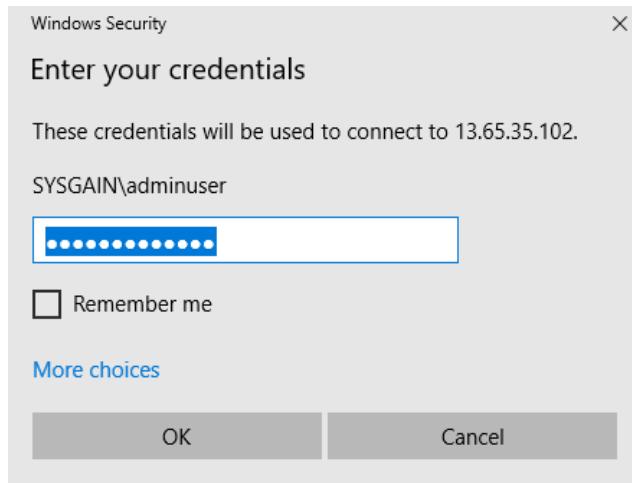
```
Administrator: Command Prompt
C:\Users\adminuser>cd C:\Users\chef-repo
C:\Users\chef-repo>cd cookbooks
C:\Users\chef-repo\cookbooks>knife cookbook upload DynatraceOneAgent
Uploading DynatraceOneAgent [0.1.0]
Uploaded 1 cookbook.

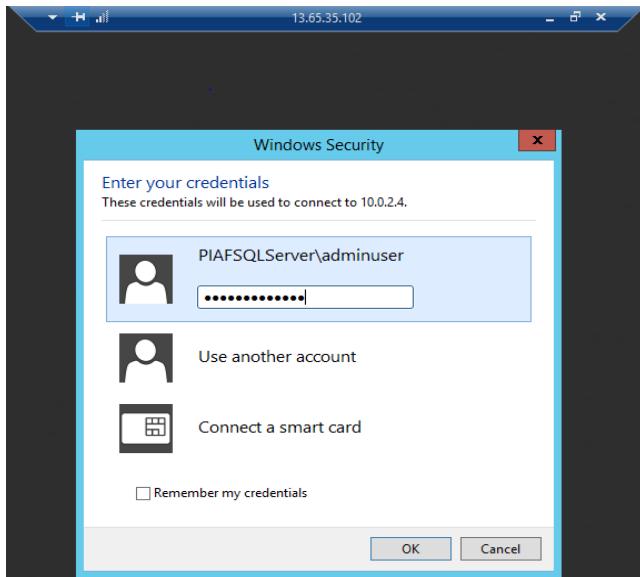
C:\Users\chef-repo\cookbooks>knife client list
10.0.1.4
10.0.2.4
10.0.4.4
bastionserverz7yo2.southcentralus.cloudapp.azure.com
orguser-validator
pidadnsw7yo2.southcentralus.cloudapp.azure.com
wsclientz7yo2.southcentralus.cloudapp.azure.com

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

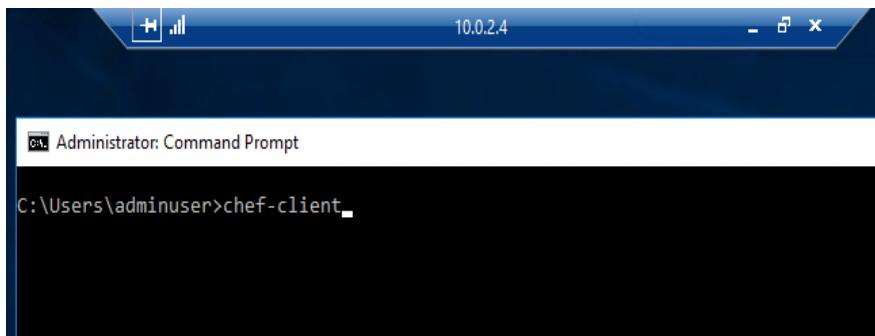
C:\Users\chef-repo\cookbooks>
```

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





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



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

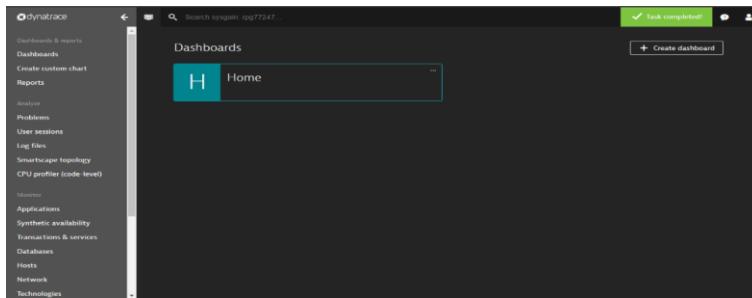
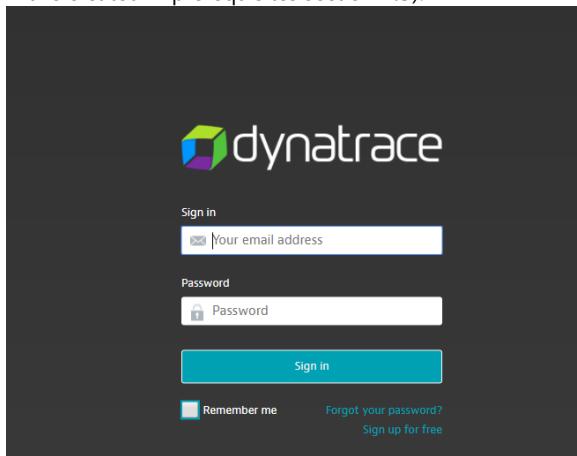
```
- install version latest of package DynatraceOneAgent
* windows_service[Dynatrace OneAgent] action restart[2017-08-16T14:10:56+00:00] INFO: Processing windows_service[Dynatrace OneAgent] action restart (DynatraceOneAgent::oneagent-windows line 28)
[2017-08-16T14:11:08+00:00] INFO: windows_service[Dynatrace 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, there's a sidebar with various monitoring categories like Dashboards & reports, Reports, Analyze, Problems, User sessions, Log files, Smartscape topology, CPU profiler (code-level), Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, and Network technologies. The main area is titled "Hosts" and shows a table for "All hosts". It lists one host: "PIDAVMServecysgainiot.com" which is "running". The table includes columns for Name, State, CPU usage, Memory usage, Disk latency, and Network traffic. Below the table, there are filters for State (Running) and Type (Azure VM), and a Data centers section showing Redmond, United States.

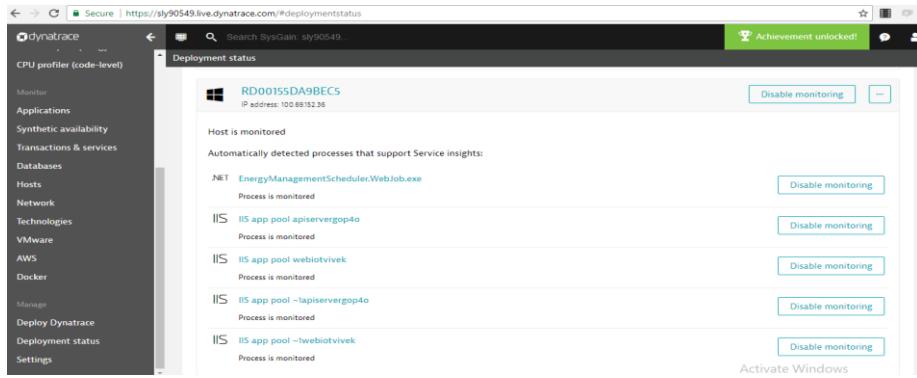
Navigate to **Deployment status** on the left pane of your dashboard page.

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

The screenshot shows the Dynatrace Deployment status dashboard. The left sidebar includes options like Monitor, Applications, Synthetic availability, Transactions & services, Databases, Hosts, Network, Technologies, VMware, AWS, Docker, Manage, Deploy Dynatrace, Deployment status, and Settings. The main dashboard shows "6 hosts" and lists three hosts with monitoring issues:

- adServer.sysgainiot.com**: IP address 10.0.1.4. Status: Host is monitored. Dynatrace OneAgent is up-to-date on version 1.125. It lists three processes: Microsoft.ActiveDirectory.WebServices.exe, WaAppAgent.exe, and WindowsAzureGuestAgent.exe. All three processes are marked as "Process isn't monitored" with a yellow warning icon and a note to "Restart this process to gain full visibility into critical process- and service-level metrics." There is a "Disable monitoring" button next to each process entry.
- Another host**: Status: Host is monitored. Dynatrace OneAgent is up-to-date on version 1.125. It lists three processes: Microsoft.ActiveDirectory.WebServices.exe, WaAppAgent.exe, and WindowsAzureGuestAgent.exe. All three processes are marked as "Process isn't monitored" with a yellow warning icon and a note to "Restart this process to gain full visibility into critical process- and service-level metrics." There is a "Disable monitoring" button next to each process entry.
- Dynatrace Security Gateways**: Status: Host is monitored. Dynatrace OneAgent is up-to-date on version 1.125. It lists three processes: Microsoft.ActiveDirectory.WebServices.exe, WaAppAgent.exe, and WindowsAzureGuestAgent.exe. All three processes are marked as "Process isn't monitored" with a yellow warning icon and a note to "Restart this process to gain full visibility into critical process- and service-level metrics." There is a "Disable monitoring" button next to each process entry.

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



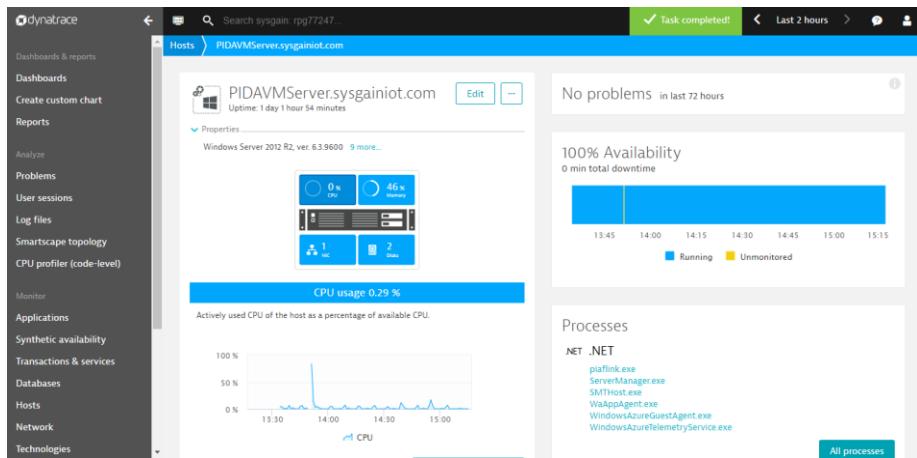
The screenshot shows the Dynatrace web interface under the 'Monitor' section. On the left, a sidebar lists various monitoring categories like Applications, Databases, and Hosts. The main content area is titled 'Deployment status' and shows a host named 'RD00155DA9BEC5' with its IP address as 100.69.132.38. It displays a list of automatically detected processes that support Service insights:

- .NET EnergyManagementScheduler.WebJob.exe (Process is monitored)
- IIS IIS app pool apiservergop4o (Process is monitored)
- IIS IIS app pool webbiotivivek (Process is monitored)
- IIS IIS app pool -apiservergop4o (Process is monitored)
- IIS IIS app pool -twebbiotivivek (Process is monitored)

Each process entry includes a 'Disable monitoring' button. At the bottom right of the main area, there is a link 'Activate Windows'.

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 web interface under the 'Monitor' section. The left sidebar shows the navigation path 'Hosts > PIDAVMServer.sysgainiot.com'. The main content area displays the host's properties and availability. Key information shown includes:

- Uptime:** 1 day 1 hour 54 minutes
- Windows Server 2012 R2, ver. 6.3.9600**
- Availability:** 100% Availability, 0 min total downtime
- CPU usage:** 0.29% (Actively used CPU of the host as a percentage of available CPU)
- Processes:** A list of running .NET processes including: psw.exe, serverManager.exe, SMTHost.exe, WaAppAgent.exe, WindowsAzureGuestAgent.exe, and WindowsAzureTelemetryService.exe.

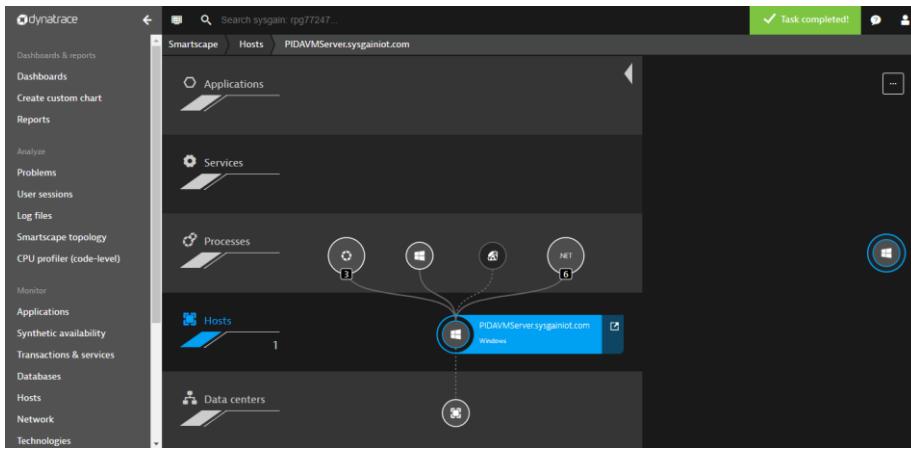
15. Click on “**All processes**”, to view the process details running on the host.

The screenshot shows the Dynatrace interface with the left sidebar menu expanded. The 'Hosts' section is selected. On the right, a table titled 'Processes' lists various system processes. The columns include Process, Type, CPU, Memory, Traffic, Retransmissions, and Connectivity. Key processes listed include Deep Security Agent, OneAgent log analytics, Windows System, ServerManager.exe, OneAgent network monitoring, Remote Desktop Connection, plalink.exe, OneAgent monitoring extensions, oneagentupdate.exe, WindowsAzureTelemetryService.exe, SMTHost.exe, chef-client, and WaAppAgent.exe. The 'CPU' column shows usage percentages ranging from 0% to 4.51%, and the 'Memory' column shows sizes from 0 B to 41.6 MB.

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 'Hosts' section selected. A host named 'PIDAVMServer.sysgainiot.com' is highlighted. The 'Properties' section displays the host's uptime as '1 day 2 hours 1 minute' and its version as 'Windows Server 2012 R2, ver. 6.3.9600'. Below this, there is a 'Smartscape view' button. The main area shows a 'No problems in last 72 hours' message and a '100% Availability' bar chart indicating '0 min total downtime' from 14:00 to 15:00. A legend at the bottom of the chart shows 'Running' in blue and 'Unmonitored' in yellow. The bottom of the screen shows a 'Processes' section with a 'CPU usage 0.21%' bar chart and a note: 'Actively used CPU of the host as a percentage of available CPU.'



### 7.1.1. Installing Dynatraceoneagent To Web Application (PaaS Environment)

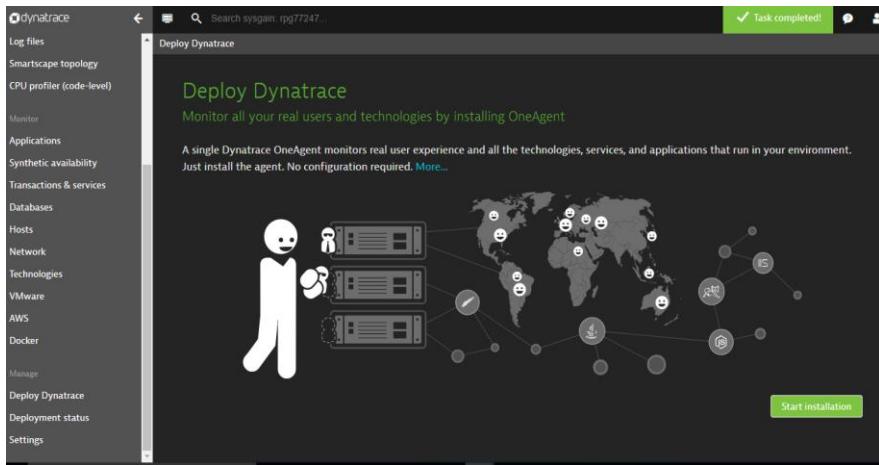
Azure Web Apps is a service provided by Microsoft Azure that gives you the option of deploying and auto-scaling applications and services. Using a predefined Azure site extension, you can modify your deployment by supplying additional resources or packages.

#### Generate a PaaS token:

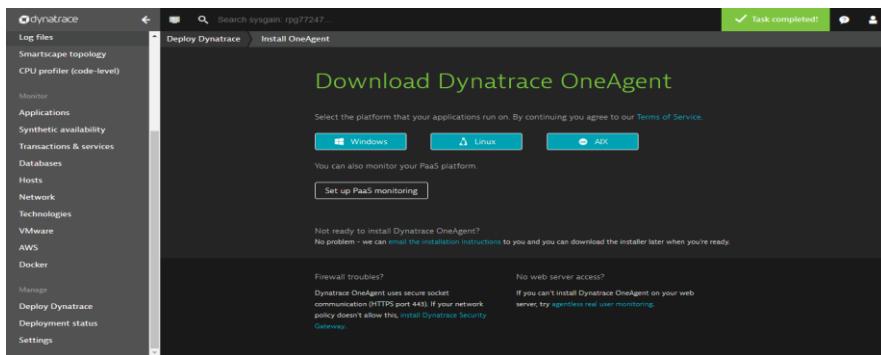
The first step is to get your environment ID and generate a PaaS token for your Dynatrace environment. This information is required so we can map your Azure account to your Dynatrace account.

To get your Dynatrace environment ID and PaaS token:

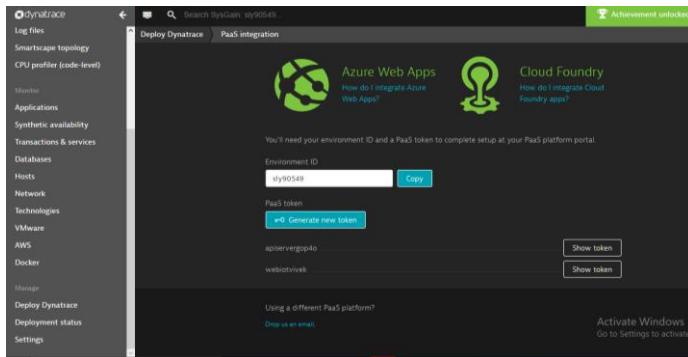
1. Login with your [Dynatrace account](#).
2. Select Deploy Dynatrace from the navigation menu.



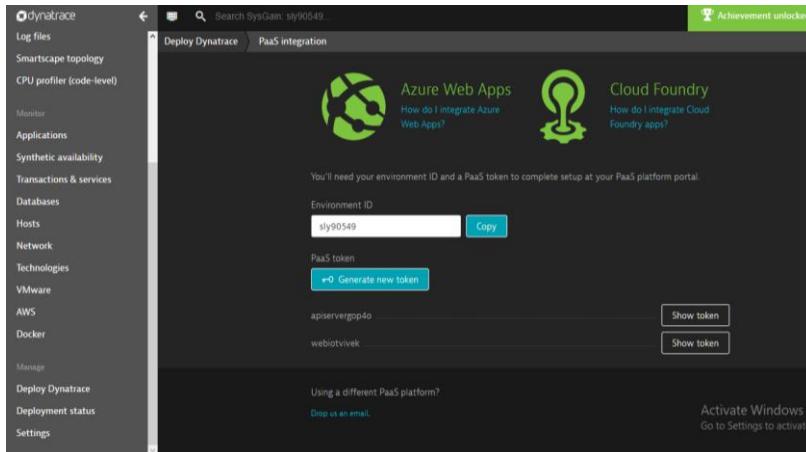
3. Click **Setup PaaS monitoring**.



- 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 PaaS token for token name "webiotivivek".

- 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

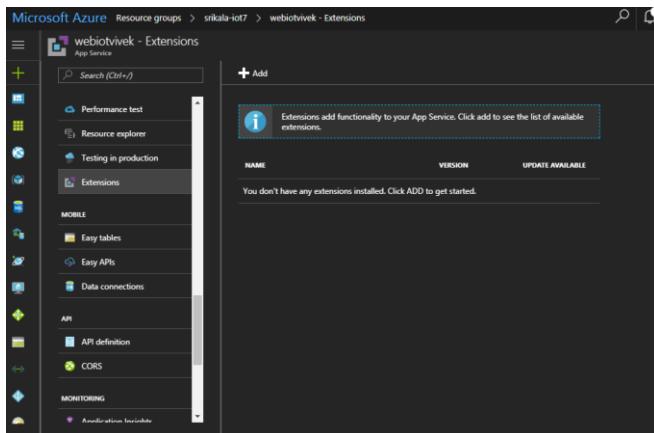
- Now, open **portal.azure.com** in a new browser window.
- Navigate to the web app in the resource group you want to monitor.
- From **Settings**, select **Application Settings**. Then, scroll down to the App Settings area and add two new **Key/Value** pairs:
- DT\_TENANT**: Your environment ID, as 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
DT_TENANT	sly90549	<input type="checkbox"/>
DT_API_TOKEN	3o2WgxoYSH6-9y5NX2GS-	<input type="checkbox"/>

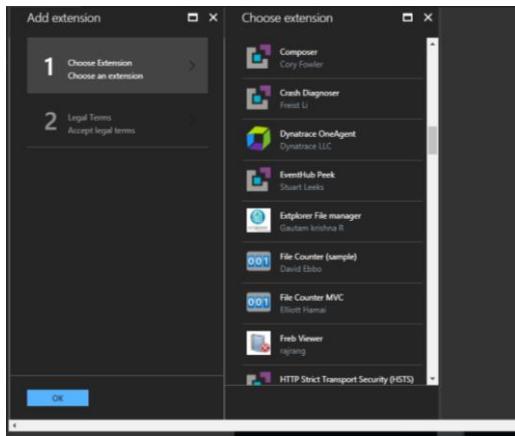
## **Install the Dynatrace Azure site extension**

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**.



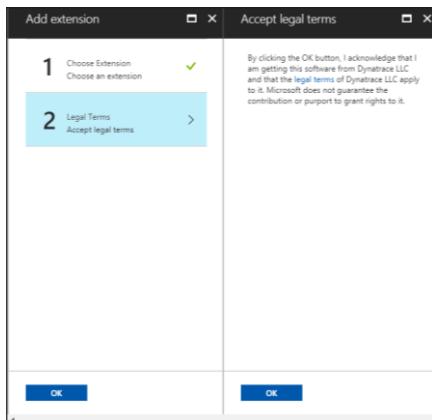
5. Scroll through the list until you find **Dynatrace OneAgent**. Note that entries are not ordered alphabetically. <https://help.dynatrace.com/images/content/infrastructure-monitoring/paas/extension.png>



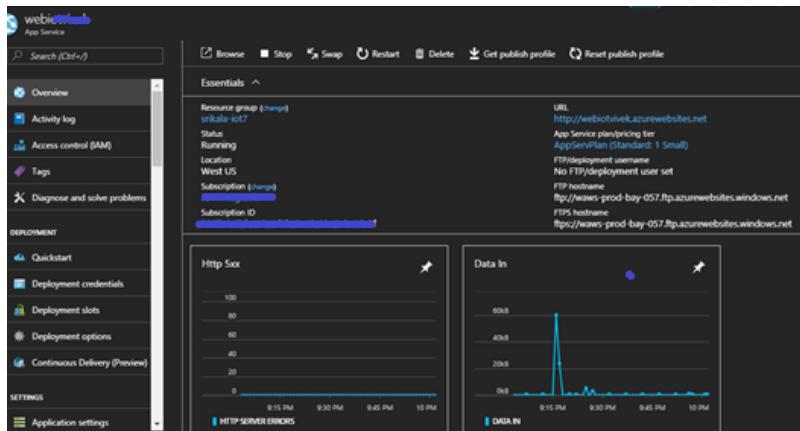
The screenshot shows the 'Extensions' blade in the Azure portal for the 'webiotiwek' app service. The sidebar includes options like Performance test, Resource explorer, Testing in production, and Extensions (which is selected). The main area displays the 'Add' button and a message: 'Extensions add functionality to your App Service. Click add to see the list of available extensions.' A table lists the installed extension:

NAME	VERSION	UPDATE AVAILABLE
Dynatrace OneAgent	1.15.121	No

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



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



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

Commented [UD34]: numbering missing

Commented [KO35R34]: updated

The screenshot shows the Dynatrace application monitoring interface. 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 two services: one named "IIS app pool ~webiotivivek" with a response time of 571 ms, failure rate of 0 %, and requests per minute at 2 /min; and another named "webiotivivek" with a response time of 3.6 ms, failure rate of 0 %, and requests per minute at 1 /min. A search bar at the top is set to "Search SysGain\_sly0549...". A green banner at the top right says "Achievement unlocked! Last 2 hours".

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

The screenshot shows the "Application settings" section of the Azure App Service settings. The left sidebar lists SETTINGS, Application settings (which is 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 pane shows a table of application settings:

Setting	Value	Slot setting	...
restServer	https://apiserverw4jil.azurewebsites.net/	<input type="checkbox"/>	...
b2cApplicationId	9e82abb2-c190-4ae2-b576-7d0e63fc9e1	<input type="checkbox"/>	...
signinPolicyName	B2C_1_singpolicy2	<input type="checkbox"/>	...
signinSignUpPolicyName	B2C_1_supolicy2	<input type="checkbox"/>	...
editProfilePolicyName	B2C_1_peditpolicy2	<input type="checkbox"/>	...
tenantName	testiot22.onmicrosoft.com	<input type="checkbox"/>	...
redirect_uri	https://webiotapp.azurewebsites.net/#/dashboard	<input type="checkbox"/>	...
DT_TENANT	rpg77247	<input type="checkbox"/>	...
DT_API_TOKEN	v81HKAGE56-77rP4lWe8H	<input type="checkbox"/>	...

Below the table, there is a "Key" input field, a "Value" input field, and a "Slot setting" checkbox. A note says "The connection string values are hidden Show connection string values".

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

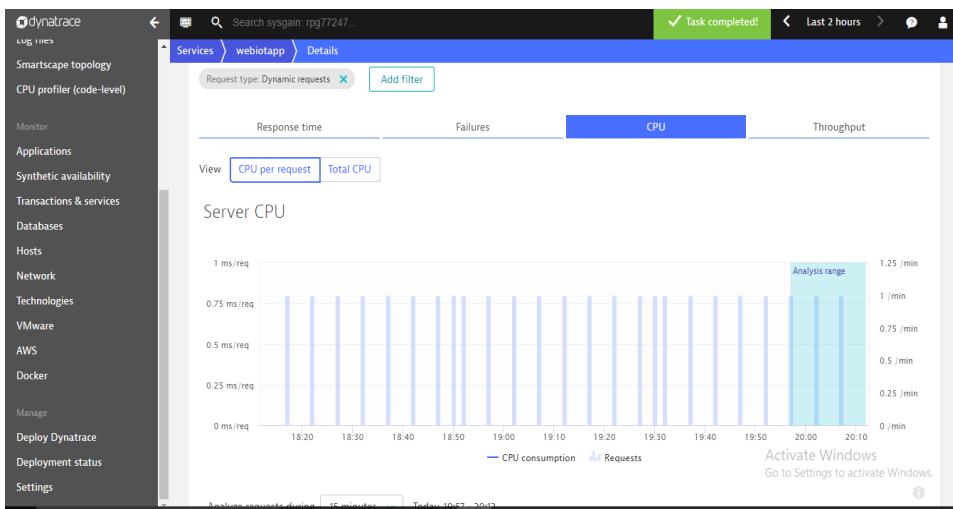
The screenshot shows the Dynatrace Services dashboard. On the left, a sidebar lists various monitoring categories like Dashboards & reports, Reports, Analyze, and Monitor. The main area displays a table titled "All monitored services" with two entries:

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

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

The screenshot shows the Dynatrace service details for "IIS ~webiotapp". The top navigation bar includes "Services" and the service name. The main content area includes sections for "Properties and tags", "Dynamic web requests", and "Understand dependencies". In the "Dynamic web requests" section, there are four key metrics displayed:

- Response time: 81.9 ms
- Failure rate: 0 %
- Throughput: 1/min
- CPU: Not explicitly shown but likely included in the "Throughput" metric



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

No hotspots detected

Understand dependencies Today, 18:18 - 20:18

Understand all dependencies and response time contributions

**View service flow**

Understand which user actions and related services are dependent on this service

Analyze backtrace

No events Today, 18:18 - 20:18

Activate Windows Go to Settings to activate Windows

Showing service flow of requests to 'webiotapp'

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

Add filter

**View PurePaths**

**show more**

webiotapp

Avg. response time 779 ms

Requests 26

Failed requests 0

See every single request in PurePath view

No service selected

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

Activate Windows Go to Settings to activate Windows

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

The screenshot shows the Dynatrace web interface. On the left is a dark sidebar with a list of monitoring categories: 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 content area has a header 'Services > webiotapp > Details > Backtrace'. Below the header is a search bar with the placeholder 'Search sysgain.rpg77247...'. A green button on the right says 'Task completed!'. The main content area displays a 'Service-level backtrace of requests to 'webiotapp''. It shows a timeline from 'Today, 18:20 - 20:20 (2 Hours)' with a 'Apply' button. An 'Add filter' button is also present. A descriptive text below the timeline states: 'The services and applications listed below make calls to this service. The tree view represents the sequence of services and application user actions that led to this service call, beginning with the page load or user action in the browser that triggered the sequence. Click to see which specific requests and user actions called this service'. Below this text is a tree view starting with 'Incoming requests to this service' and listing 'ASP .NET IIS app pool webiotapp'. At the bottom right of the main content area, there is 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"

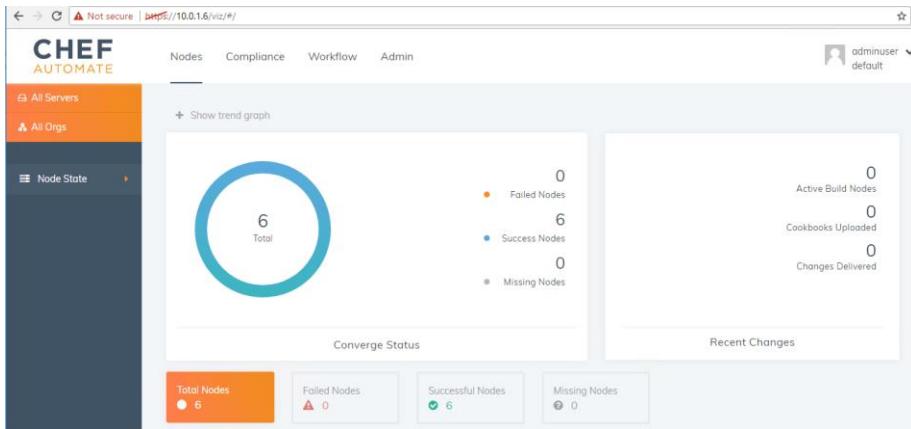
The screenshot shows the Azure portal interface for the resource group 'srikala-iot8'. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, and Automation script. Below that is a Monitoring section. The main area is titled 'Essentials' and shows deployment details: Subscription name (changed), IoT Integration, Deployment status (12 Succeeded). A table lists 66 items, filtered by type (Virtual machine) and location (South Central US). The 'chefworkstation' row is highlighted with a blue selection bar.

This screenshot shows the detailed view for the 'chefworkstation' virtual machine. The left sidebar has options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Availability set, Disks, Extensions, Network interfaces, Size, Backup, and Properties. The main panel shows the machine's configuration: Resource group (changed), Status (Running), Location (South Central US), Subscription (changed), and Subscription ID. A callout box highlights the 'Public IP address' field, which contains '13.65.146.32'. Below this, it shows the virtual network (MyVNET/subnet1) and DNS name (wsclient7kbp.southcentralus.cloudapp.azure.com). At the bottom, there are three performance charts: 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.

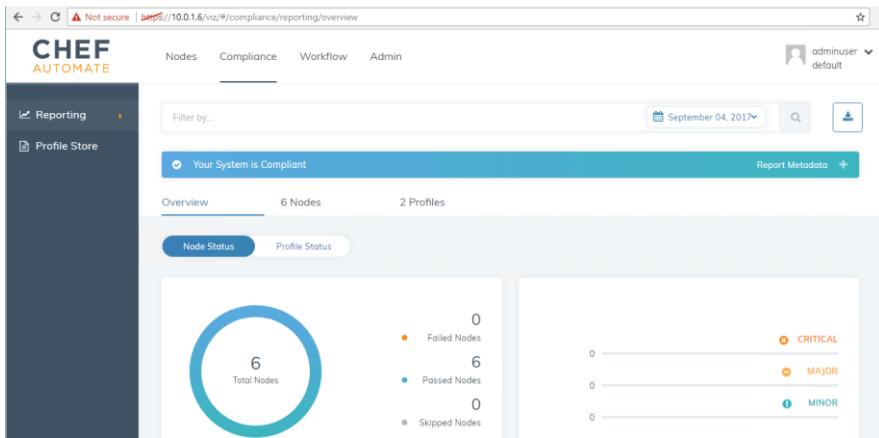


Converge	Node Name	Check-in	Uptime	Platform	Environment
✓	odserver	3 days ago	on hour	windows	_default
✓	bastionserver	3 days ago	2 hours	windows	_default
✓	piadfasqlserver	3 days ago	on hour	windows	_default
✓	pibaserver	3 days ago	on hour	windows	_default
✓	trendserver	3 days ago	2 hours	centos	_default
✓	workstation	3 days ago	on 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

Nodes	Platform	Environment	Last Scan	Control Failures
ADServer	Windows Server 2016 ...	_default	3 days ago	PASSED
workstation	Windows Server 2012 ...	_default	3 days ago	PASSED
bastionserver	Windows Server 2012 ...	_default	3 days ago	PASSED
piafdasqlserver	Windows Server 2016 ...	_default	3 days ago	PASSED
piboserver	Windows Server 2012 ...	_default	3 days ago	PASSED
trendserver	centos	_default	3 days ago	PASSED

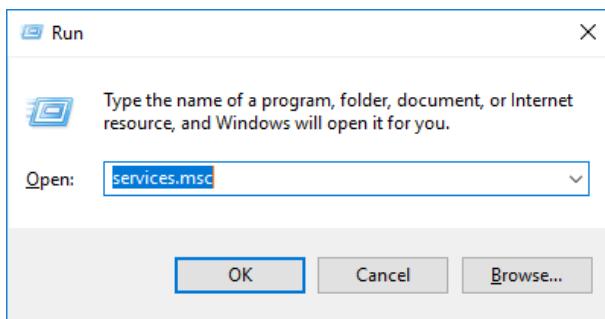
Select any one node to view the failed or passed controls of nodes individually

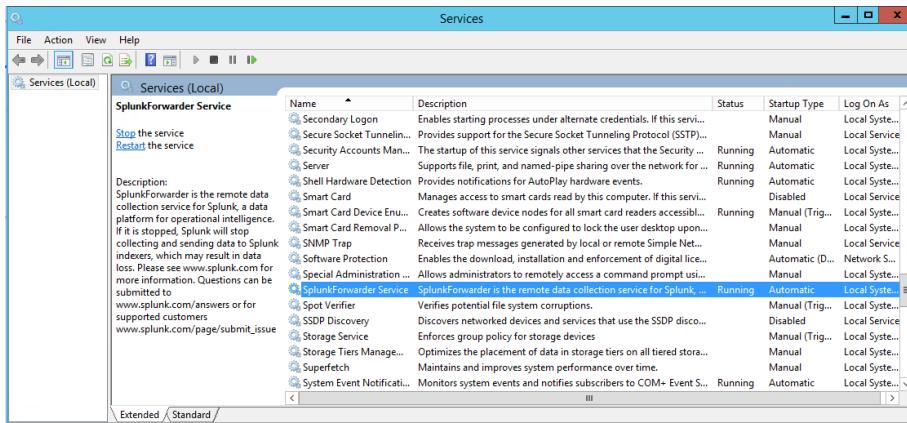
### Splunk Universal Forwarder Installation Using Chef Automate:

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.

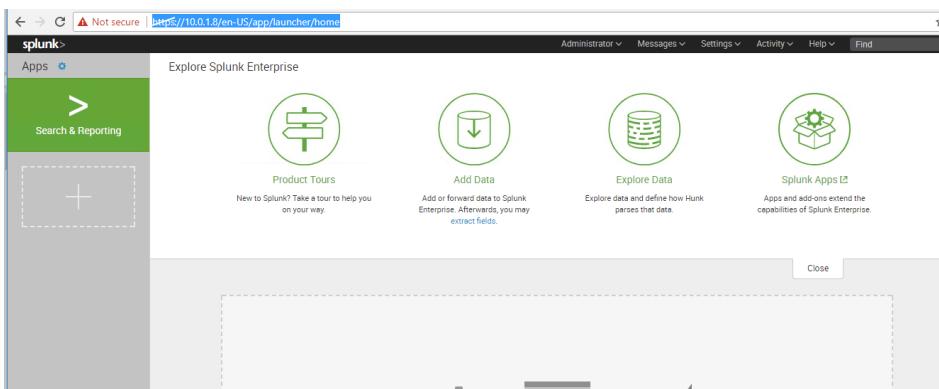
In our system Splunk server getting all windows logs from client machines automatically, for this we have installed splunk-forwarder using chef automate in every windows server. To view the logs in splunk server.

Step1:

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

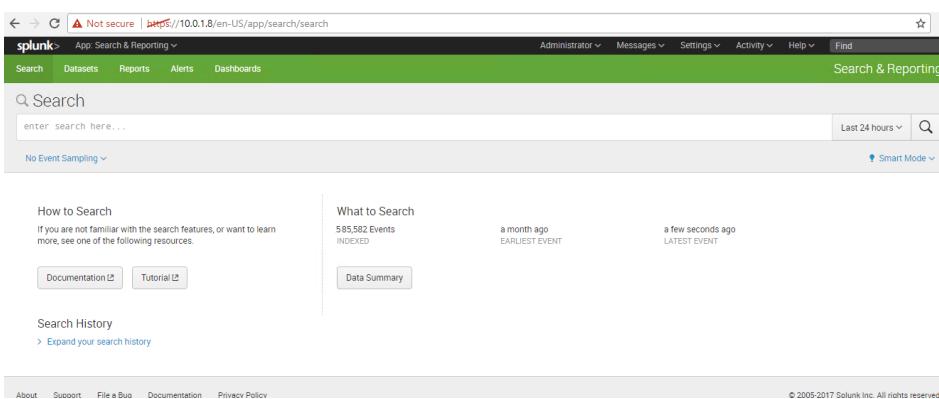
Username: admin

Password: Password@1234



Step2:

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



### 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 a search bar at the top with the query "host='bastionserver'".

**Screenshot 1 (Top):** This screenshot shows the search interface with a green header bar. Below the search bar, there's a "Search & Reporting" section. The search results table has one visible row:

Time	Event
8/30/17 12:21:25 PM 12:21:25 000 PM	08/30/2017 12:21:25 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Show all 61 lines host = bastionServer   source = WinEventLog:Security   sourcetype = WinEventLog:Security

**Screenshot 2 (Bottom):** This screenshot shows a more detailed view of the search results. It includes a timeline at the bottom and a larger table with two rows of data. The table columns are "Time" and "Event".

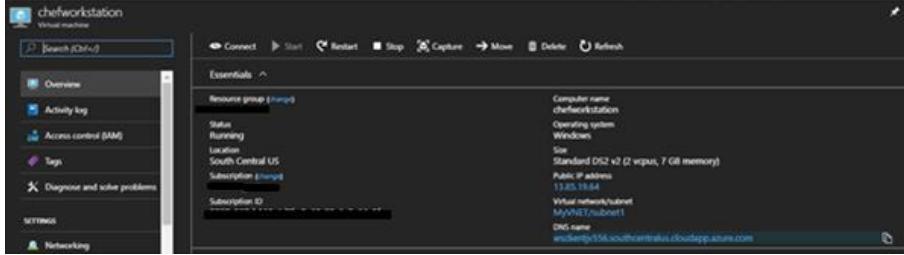
Time	Event
8/30/17 12:21:25 PM 12:21:25 000 PM	08/30/2017 12:21:25 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Show all 61 lines host = bastionServer   source = WinEventLog:Security   sourcetype = WinEventLog:Security
8/30/17 12:21:04 000 PM 12:21:04 000 PM	08/30/2017 12:21:04 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Show all 61 lines host = bastionServer   source = WinEventLog:Security   sourcetype = WinEventLog:Security

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.

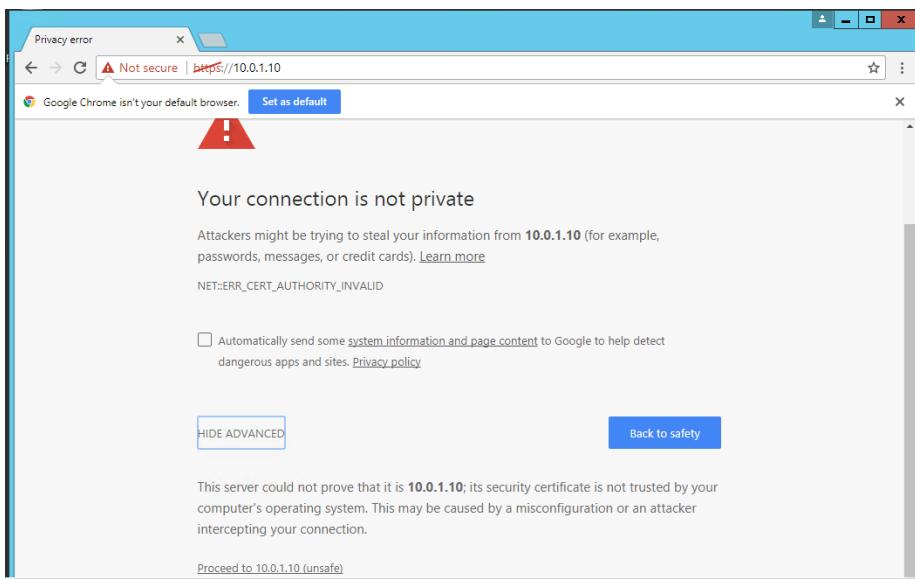
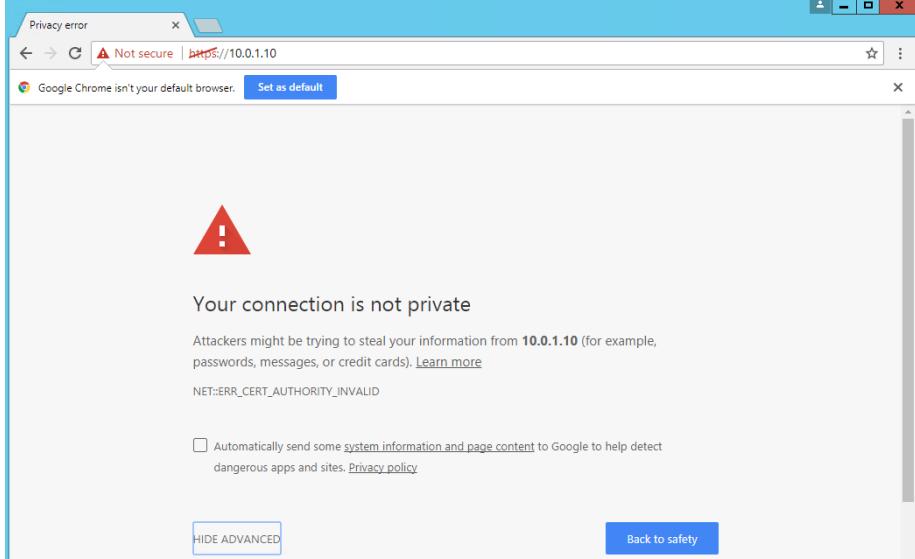


Once login open Browser and enter the TrendMicro IP address, which we get from output section of IOT ARM Template.

A screenshot of the Microsoft Azure portal showing the 'Microsoft.Template' deployment settings. The 'Variables' section lists the following variables:

Variable	Value
WORKSTATIONFQDN	wsclientjv556.southcentralus.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	fortigatejv556
AZURESQLENDPOINT	sqlserverjv556.database.windows.net
AZURESQLDBNAME	azuredb
AZURESQLUSERNAME	sqluser

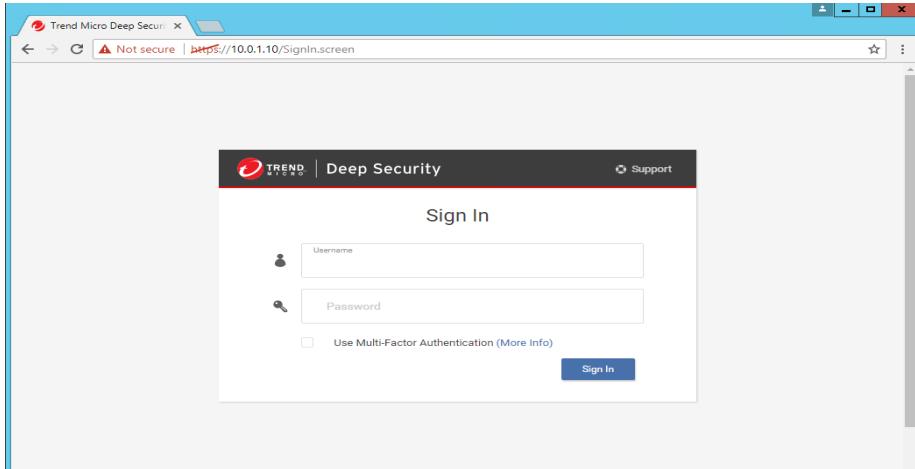
Click on "HIDE ADVANCED" and then click on "proceed to 10.0.1.10"



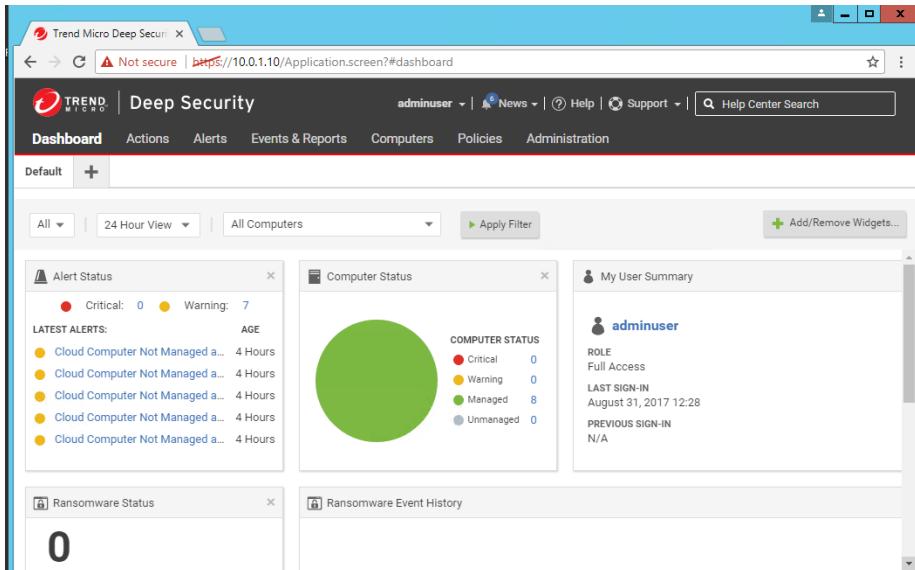
Login to Trend using the credentials.

Username: adminuser

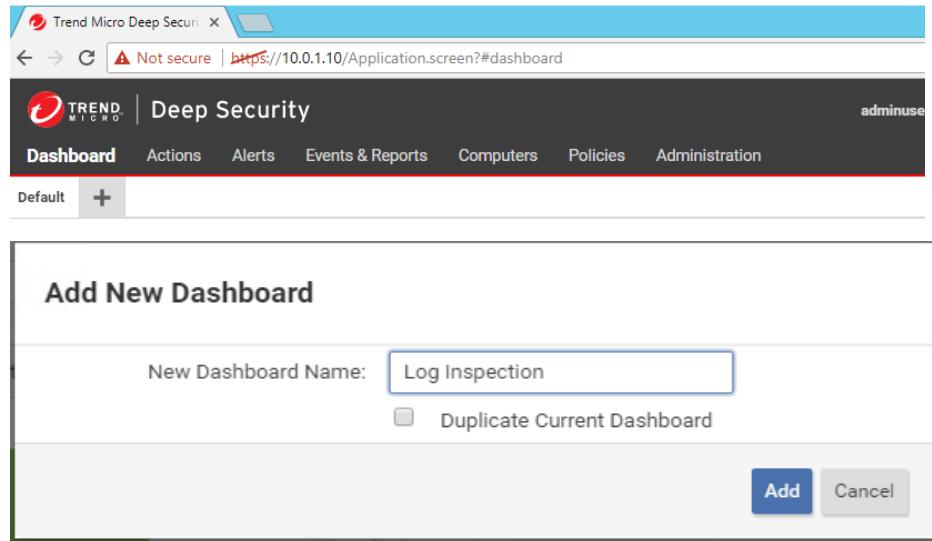
Password: Password@1234



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.

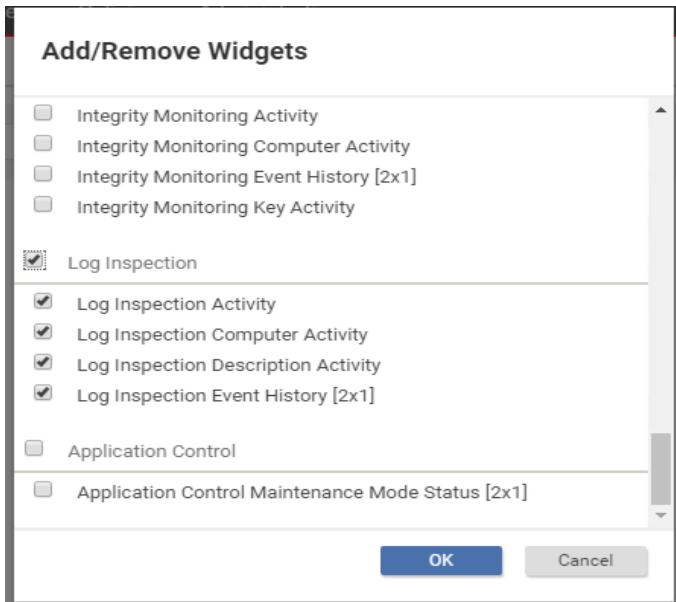


We can create our own Dashboard by clicking on "+" icon Besides Default and add the Widgets which you want to monitor.



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





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

The screenshot shows the main interface with a top navigation bar including "Default", "Log Inspection", and a "+" button. Below the bar are filter options: "All", "24 Hour View", "All Computers", and "Apply Filter". On the right is an "Add/Remove Wdg" 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", showing a single entry: "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 interface. The top navigation bar includes links for Dashboard, Actions, Alerts, Events & Reports, Computers (which is the active tab), Policies, and Administration. Below the navigation is a search bar and a toolbar with options like Add, Delete, Details, Actions, Events, Export, and Columns. A main table lists 8 computers, each with columns for Name, Description, Platform, Policy, Status, and Maintenance. All listed computers are 'Managed (Online)' and have 'N/A' in the Status column.

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

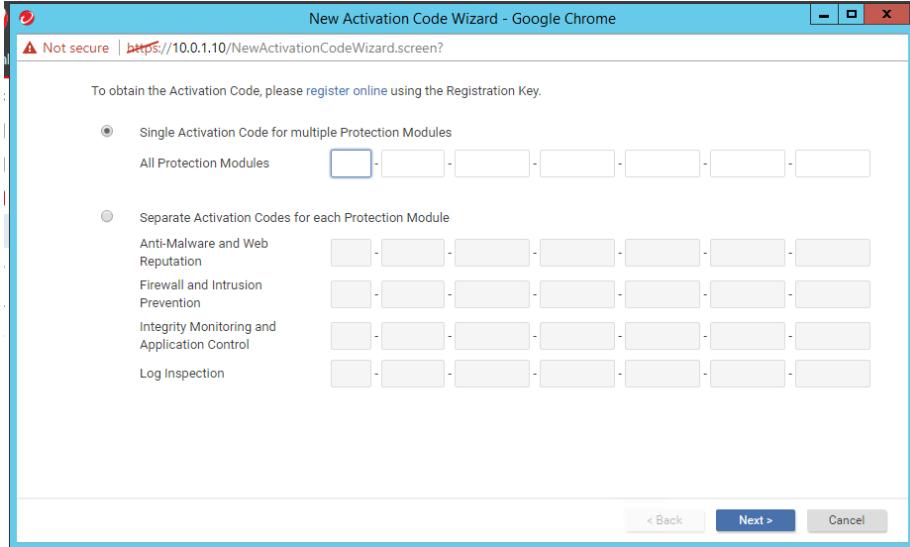
For installing the TrendMicro License, click on **Administration** from top menu.

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

The screenshot shows the Trend Micro Deep Security interface with the Administration tab selected. On the left, a sidebar lists various management options: System Settings, Scheduled Tasks, Event-Based Tasks, Manager Nodes, Licenses (which is the active tab), User Management, System Information, and Updates. The main content area displays a table of current licenses. The table has columns for Status, Type, and Expires. All listed items are 'Not Licensed'. There is a 'View Details...' button next to each row. At the bottom of the table is a button labeled 'Enter New Activation Code...'. Above the table, a note says 'License Mode: Bring your own license'.

	Status	Type	Expires	
Anti-Malware and Web Reputation	Not Licensed	N/A	N/A	<a href="#">View Details...</a>
Firewall and Intrusion Prevention	Not Licensed	N/A	N/A	<a href="#">View Details...</a>
Integrity Monitoring and Application Control	Not Licensed	N/A	N/A	<a href="#">View Details...</a>
Log Inspection	Not Licensed	N/A	N/A	<a href="#">View Details...</a>

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



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

Deep Security

Dashboard Actions Alerts Events & Reports Computers Policies Administration

adminuser | News | Help | Support | Help Center Search

Licenses

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	<a href="#">View Details...</a>
Firewall and Intrusion Prevention	Activated	Full	September 28, 2017	<a href="#">View Details...</a>
Integrity Monitoring and Application Control	Activated	Full	September 28, 2017	<a href="#">View Details...</a>
Log Inspection	Activated	Full	September 28, 2017	<a href="#">View Details...</a>

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 screenshot shows the 'Computers' section of the Trend Micro Deep Security interface. It lists eight computers, each with its name, description, platform, policy, status, maintenance schedule, and the last time a policy was successfully sent. The status column includes icons indicating managed or unmanaged status, and online/offline status.

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

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

Click on Anti-Malware from left side menu.

The screenshot shows the configuration page for computer 10.0.0.6. On the left, there's a sidebar with various monitoring and control options. The main area is divided into sections: General, Actions, and System Events. Under the General tab, there are fields for Hostname, Display Name, Description, Platform, Group, Policy, Asset Importance, and Download Security Updates From. The 'Agent' section is expanded, showing the current status as 'Managed (Online)' and a list of configuration options for Anti-Malware, Firewall, Intrusion Prevention, Integrity Monitoring, Log Inspection, and Application Control. The 'Online' dropdown is set to 'Yes'. At the bottom right are 'Save' and 'Close' buttons.

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

This screenshot shows the 'Anti-Malware' configuration page for a computer with IP 10.0.0.6. It includes tabs for General, Smart Protection, Advanced, Identified Files, and Anti-Malware Events. The Anti-Malware section is active, displaying configuration options like 'Default (Off)' for 'Configuration' and 'Off, not installed, no configuration' for 'State'. It also lists 'Real-Time Scan', 'Manual Scan', and 'Scheduled Scan' sections, each with inheritance checked and 'No Configuration' selected for 'Malware Scan Configuration'. A note at the bottom indicates 'Last Manual Scan for Malware: N/A'. At the bottom right are 'Save' and 'Close' buttons.

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**

Task(s)

- Anti-Malware
- Web Reputation
- Firewall
- Intrusion Prevention
- Integrity Monitoring

Managed (Online)  
Update of Configuration Pending (Heartbeat)  
On, Real Time  
Off, Installation pending  
Off, not installed, no rules  
Off, not installed, no rules  
Off, not installed, no rules

This screenshot shows the 'General' tab of the 'Computer' overview page for IP 10.0.0.6. It displays basic information like Hostname (10.0.0.6), Platform (Microsoft Windows Server 2012 R2 (64 bit) Build 9600), and Agent status (Managed (Online)). The 'Agent' section lists tasks such as Anti-Malware, Web Reputation, Firewall, Intrusion Prevention, and Integrity Monitoring, with their current status (e.g., 'On, Real Time').

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

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

The screenshot shows the Trend Micro Deep Security Administration interface. In the top navigation bar, there are links for Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, and Administration. Under the Administration tab, the 'Scheduled Tasks' section is selected. A table titled 'Scheduled Tasks' lists two tasks: 'Daily check for Security Updates' and 'Daily check for Software Updates'. The 'New...' button in the top left of the table header is highlighted with a red box.

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

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

General	Task Details
---------	--------------

**General Information**

Name:

Type:

Task Enabled:

**Schedule Information**

Hourly  Daily  Weekly  Monthly  Once  Only

**Daily Schedule Details**

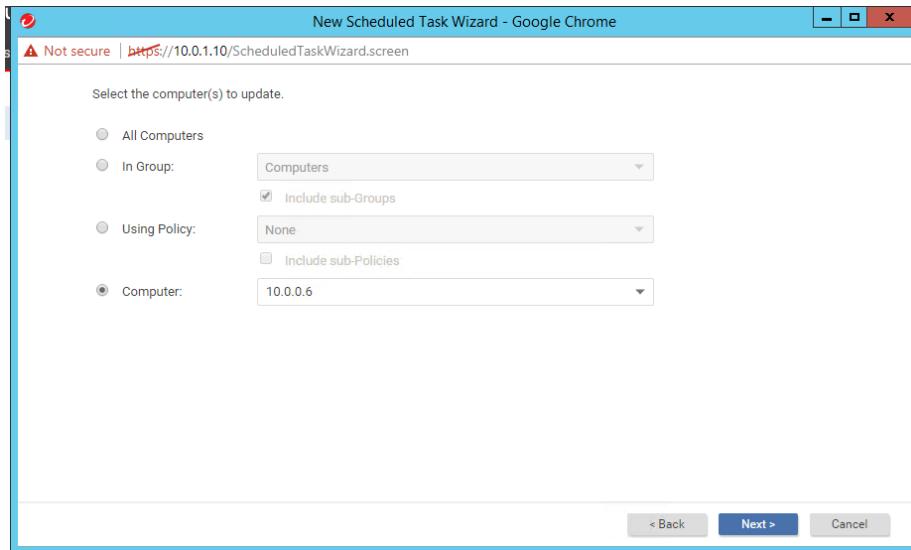
Start date:

Start time:

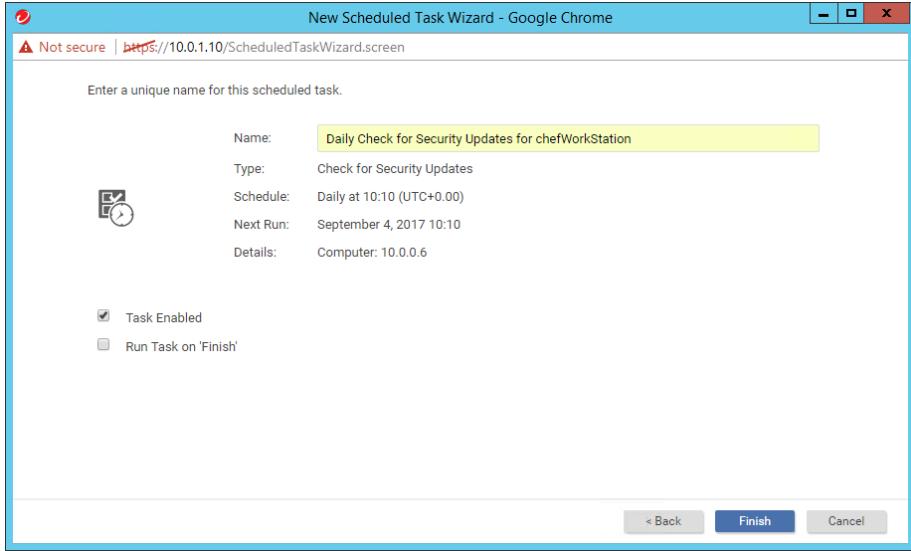
Time zone:

Every Day   
Weekdays   
Every  days

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



### Click on Finish



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

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

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

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

Performing Security Update on 1 Computer

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

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

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

Computer: 10.0.0.6

Overview General Actions System Events

System Events All No Grouping

Period: Last Hour

Computers: Computer: 10.0.0.6

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

TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...
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

General Actions System Events

System Events All No Grouping

Period: Last Hour

Computers: Computer: 10.0.0.6

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

TIME	LEVEL	EVENT ID	EVENT	TAG(S)	EVENT ORIGI...	TAR
September 4, 2017 09:03:53	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:59:59	Select All (14)	1204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:59:59	Export Selected to CSV...	273	Security Update: Security Update Check and Download Requested	Manager	10.0	
September 4, 2017 08:59:59	View	1204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:59:59	Events Retrieved	710	Events Retrieved	Agent	10.0	
September 4, 2017 08:59:59	Add Tag(s)...	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	
September 4, 2017 08:59:59	Remove Tag(s)...	276	Update: Summary Information	Manager	10.0	
September 4, 2017 08:59:59	Info	2204	Security Update: Pattern Update on Agents/Appliances Successful	Agent	10.0	

The screenshot shows the Trend System Events interface for Computer 10.0.0.6. The left sidebar contains various monitoring modules like Anti-Malware, Web Reputation, Firewall, etc. The main area displays a table of system events. The table has columns for TIME, LEVEL, EVENT ID, EVENT, TAG(S), EVENT ORIGIN, and TARGET. The data shows several entries related to security updates, such as 'Security Update: Pattern Update on Agents/Appliances Successful' and 'Security Update: Security Update Check and Download Requested'. The interface includes filters for Period (Last Hour) and Computers (Computer: 10.0.0.6), and options for View, Export, Auto-Tagging, and Columns.

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

The screenshot shows the Trend Event logs interface. It displays a file named 'System\_Events' (1) in Microsoft Excel format, which contains two rows of event data. The data is as follows:

Time	Level	Event ID	Event	Tag(s)	Event Origin	Target	Action By	Manager	Description
September 4, 2017 09:00:25	Info	273	Security Update: Security Update Check and Download Request	Manager	10.0.0.6	System	10.0.1.10		Description Omitted

Below this, another file named 'System\_Events' is shown, also in Microsoft Excel format, containing a single row of event data:

Time	Level	Event ID	Event	Tag(s)	Event Origin	Target	Action By	Manager	Description
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

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. The top navigation bar includes links for Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, and Administration. The Alerts section is currently selected. A sub-menu for Alerts offers 'Summary View' and 'By Time'. The main content area shows a message about recommendations for one computer, with details like time (September 4, 2017 06:01), last updated (September 4, 2017 06:01), severity (Warning), and computer(s) (10.0.0.5). Below this is a message about licensing for Anti-Malware and Web Reputation, which expires on September 28, 2017. The protection module's license will expire soon, and users can remove it by changing their license on the Administration > Licenses page. The timestamp for this message is August 31, 2017 12:43.

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

This screenshot shows the full alert list after clicking the 'Alerts' link. The interface includes a search bar for 'Severity' set to 'Warning'. The alert list table has columns for TIME, SEVERITY, ALERT, TARGET, and SUBJECT. The data rows show various alerts from August 31, 2017, including recommendations, protection module licensing issues, and cloud computer status notifications. At the bottom right of the alert list, there is a summary: ALERTS [12] 0.

USES:

## 1. Adding computer to deep security manager

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

## 2. Deploying protection

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

### 3. Assigning security policies

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

### 4. Keeping your protection up to date

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

### 5. Keeping informed of Deep security events

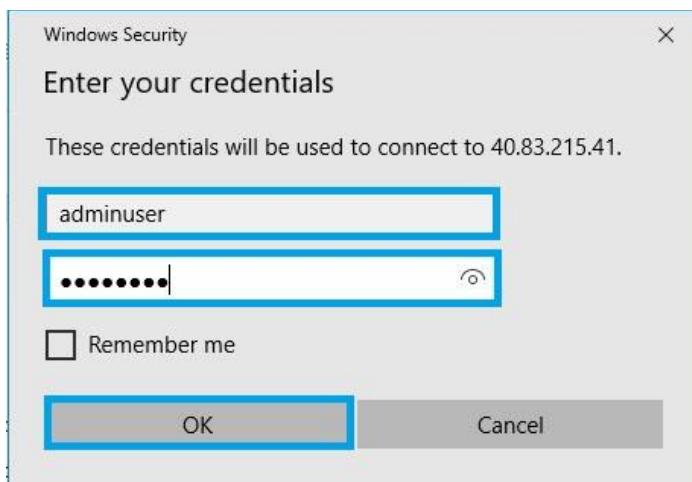
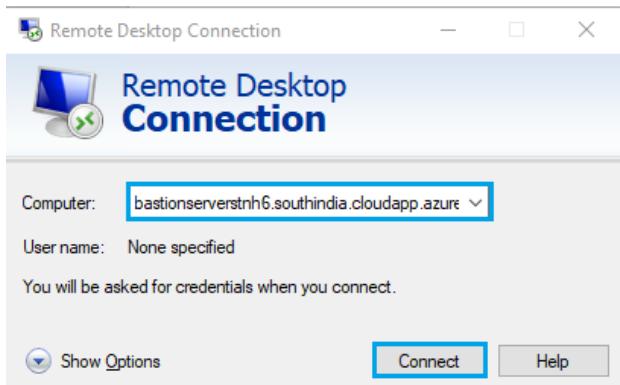
Use the customizable dashboard for quick, at-a-glance, views of the status of your Deep security system. Create scheduled Tasks to periodically send out customizable reports and set up your user account to receive notifications by email of important alerts

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

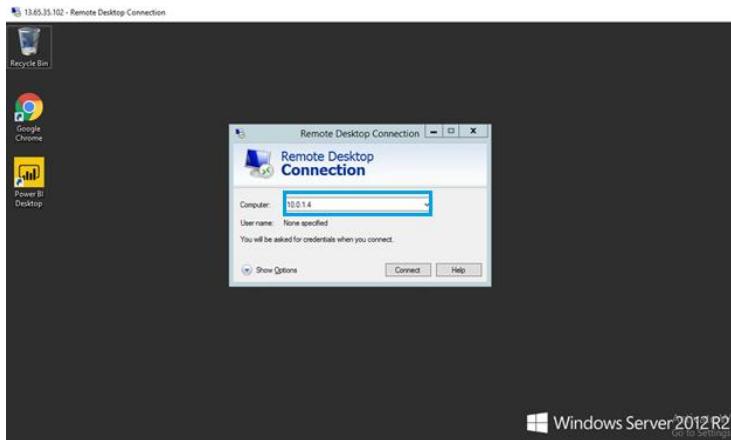
1. Login to the **Bastion Host VM** using **BASTIONFQDN** and **ADMINUSERNAME** provided in the **Outputs** section

### Outputs

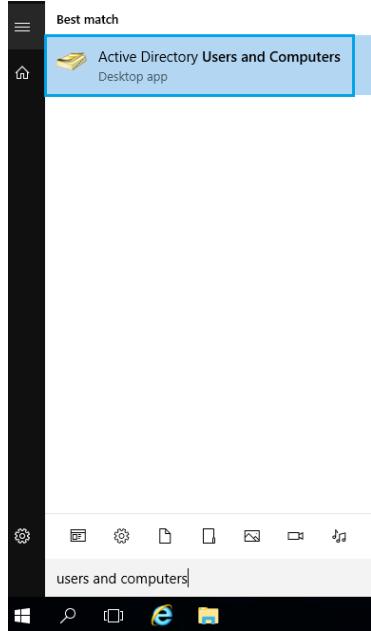
ADMINUSERNAME	adminuser	
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com	
ADSERVERIPADDRESS	10.0.1.4	



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



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



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

The screenshot shows the 'Active Directory Users and Computers' management console. The left navigation pane lists several containers: 'Saved Queries', 'sysgainiot.com' (which is expanded to show 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', and 'Users'), and 'ForeignSecurityPrincipal'. The 'Computers' folder under 'sysgainiot.com' is highlighted with a blue selection box. The right pane displays a table of computer objects:

Name	Type
bastionServer	Computer
chefworkstation	Computer
PIAFSQLServer	Computer
PIBAVMServer	Computer

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

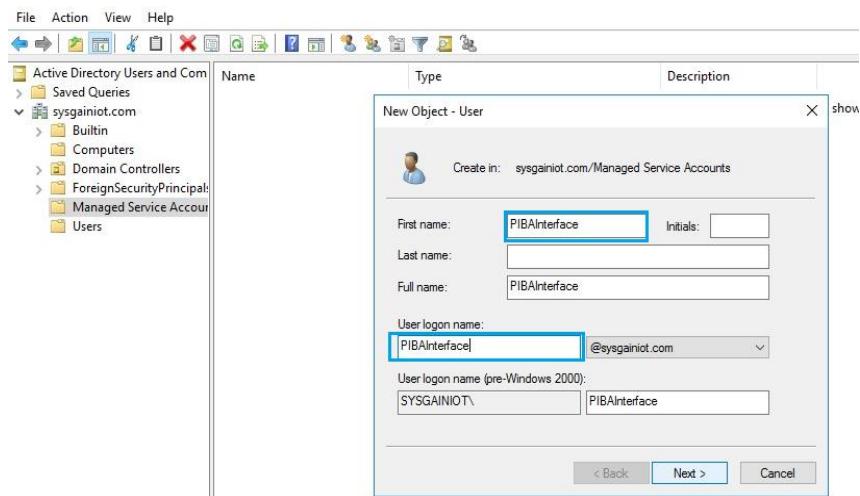
The screenshot shows the same 'Active Directory Users and Computers' interface. The 'Managed Service Account' folder under 'sysgainiot.com' is selected and has a context menu open. The 'New' option in the menu is highlighted with a blue selection box. A secondary menu appears below it, listing various object types. The 'User' option is also highlighted with a blue selection box.

- New >
- All Tasks >
- View >
- Cut
- Delete
- Rename
- Refresh
- Export List...
- Properties
- Help

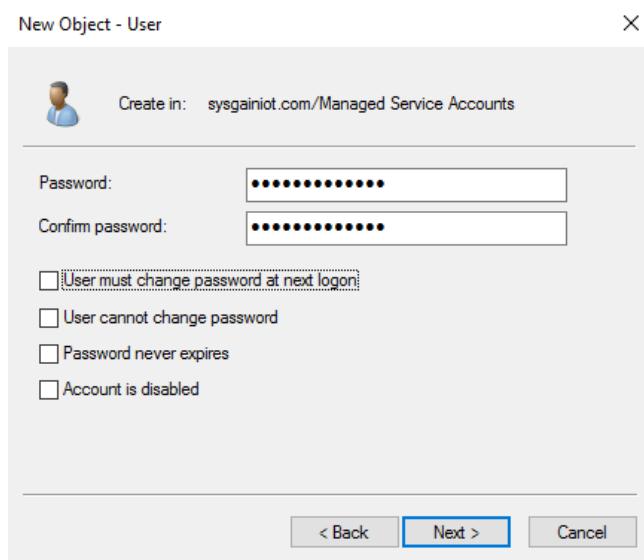
- Computer
- Contact
- Group
- InetOrgPerson
- msDS-KeyCredential
- msDS-ResourcePropertyList
- msDS-ShadowPrincipalContainer
- msImaging-PSPs
- MSMQ Queue Alias
- Printer
- User
- Shared Folder

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

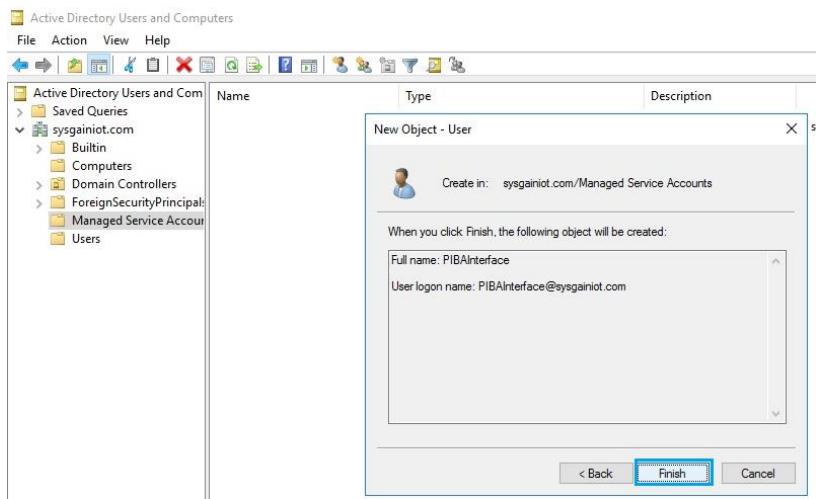
Commented [AS36]: Use the naming standard for the First name and User logon name.



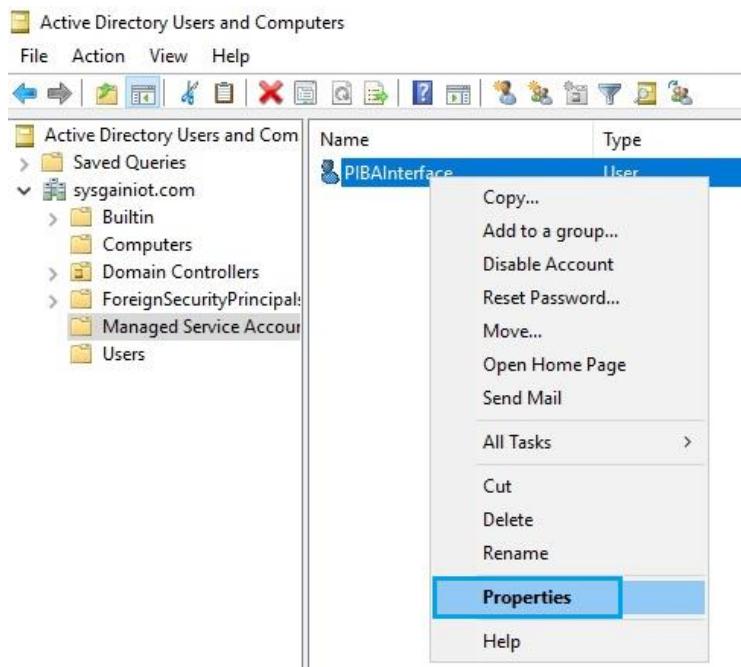
7. Enter the **Password** and uncheck **User must change password at next logon**. Click on **Next**.



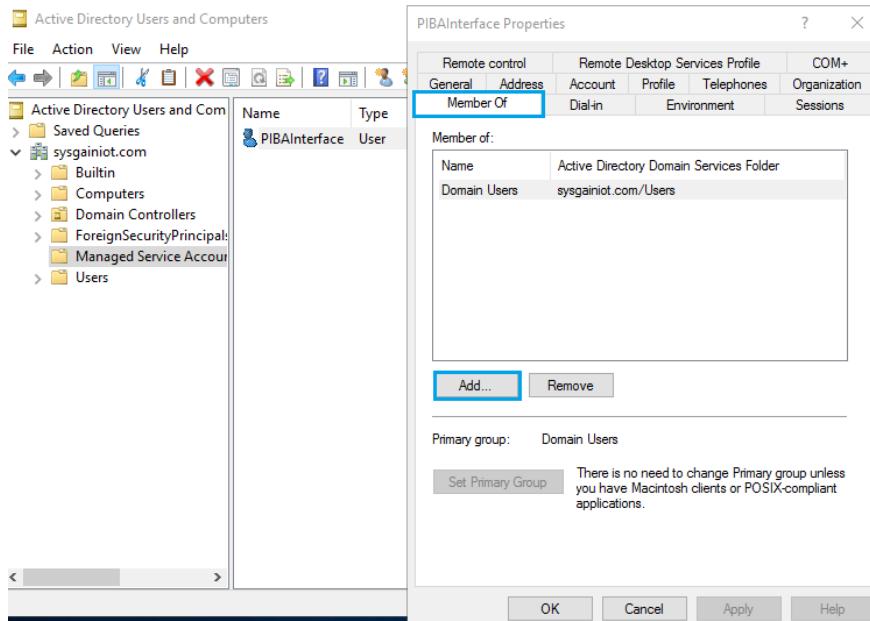
8. Click **Finish** once the object is created.



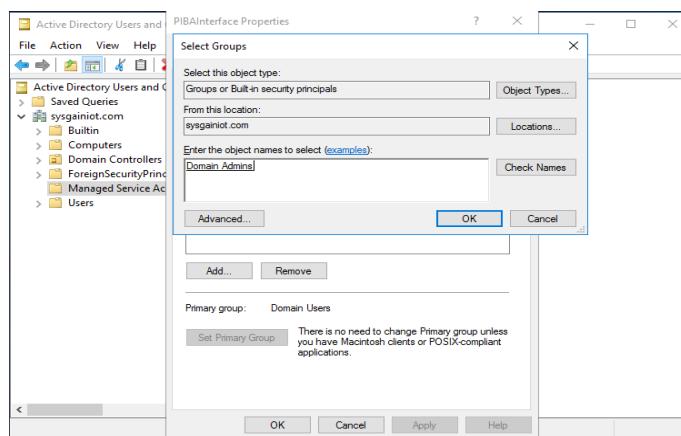
9. Check on the properties of the user created. Right click on the **PIBAInterface** and click on **Properties**.



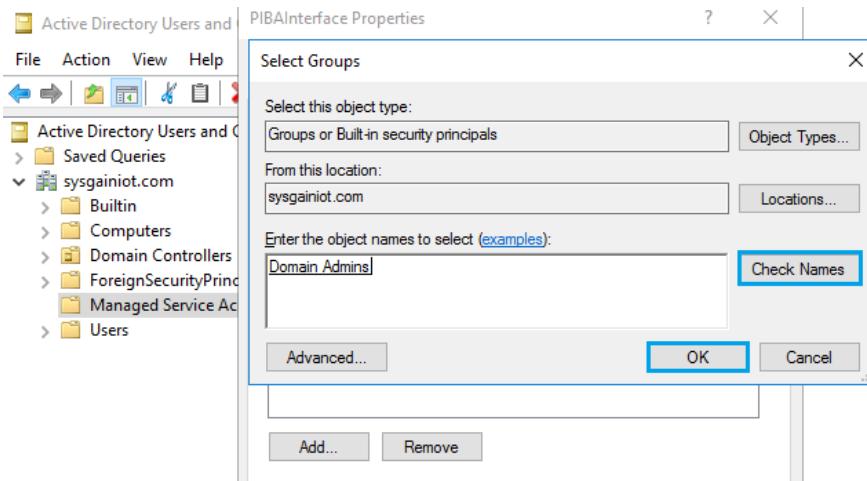
10. A popup will appear. Click on the **Member Of** tab and click the **Add** button.



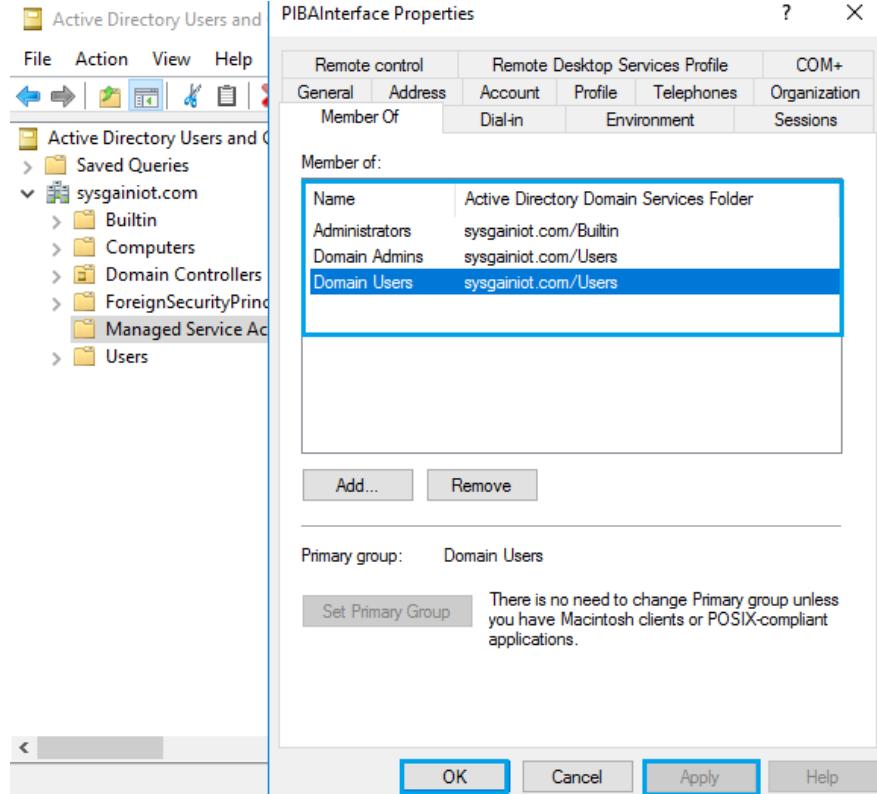
11. Enter the object name as **Domain Admins** and click on **Check Names**. It will display the Domain Admins as object names. Click on **Ok**. After that, click on **Ok** again. You will see the Domain Admin name added to the **Member of** section.



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**.



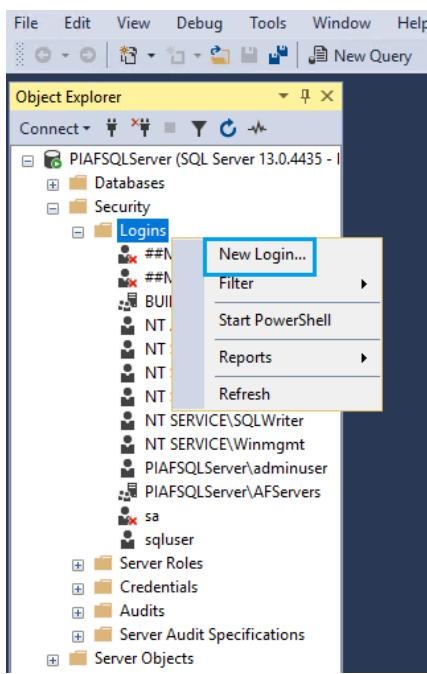
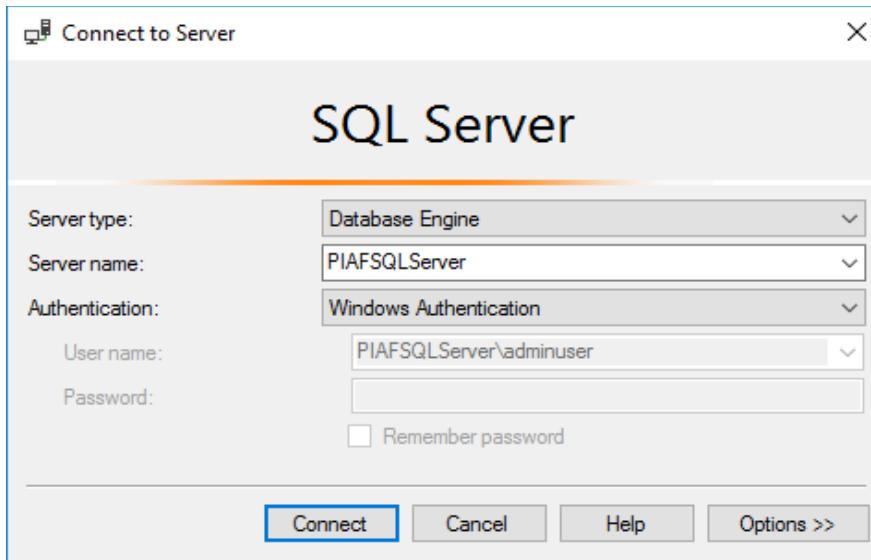
## 8.1. Create PIBA User in PIAF Server

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

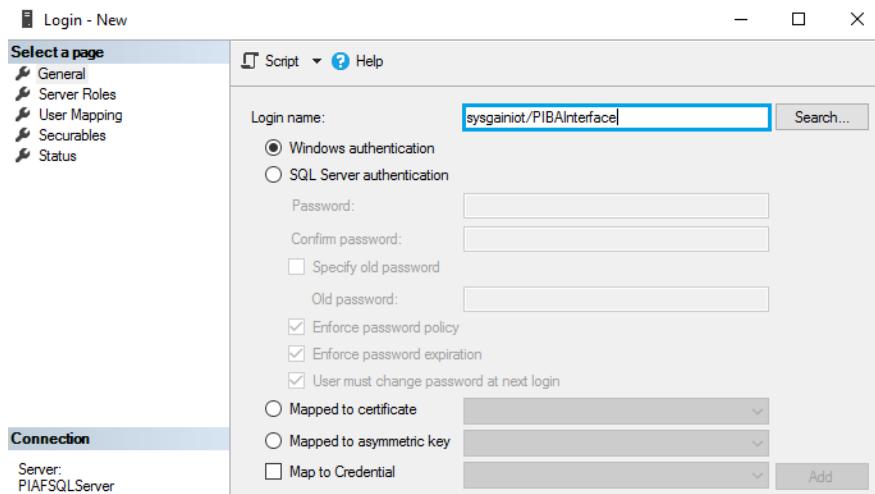
Outputs	
ADMINUSERNAME	adminuser
BASTIONFQDN	bastionserverfevs6.westus.cloudapp.azure.com
ADSERVERIPADDRESS	10.0.1.4
PIAFSQLSERVERIPADDRESS	10.0.2.4



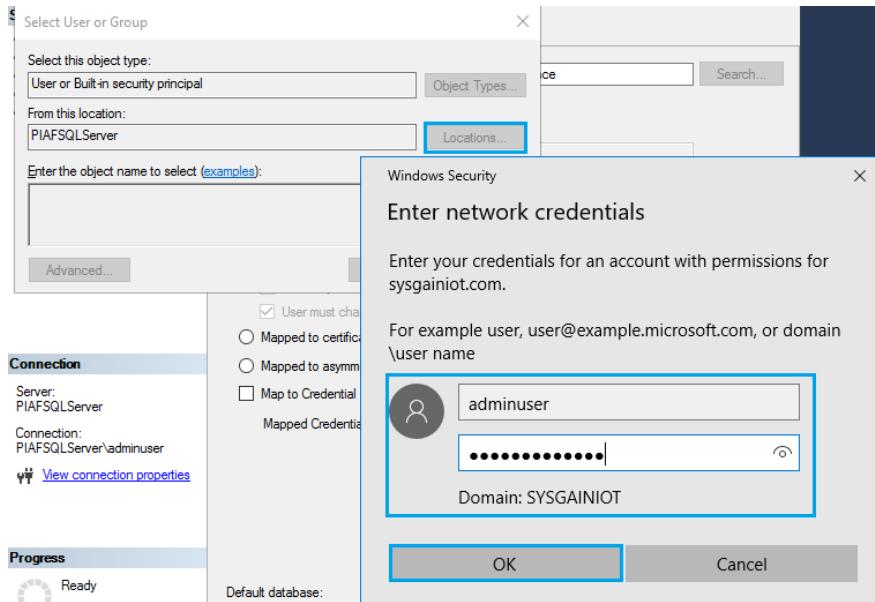
2. After logging in to the PIAF SQL Server, search for **ssms** in start menu to open the open the **SQL Server Management Studio** and create a new login by navigating to **Security** > Right-click on **Logins** and selecting **New Login**.



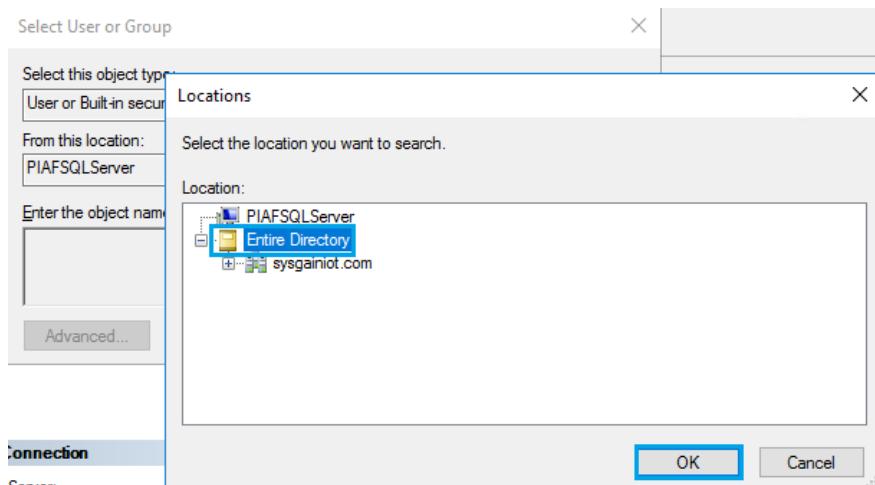
3. Give the login name as <domain name>/PIBAInterface, then click on **Search**.



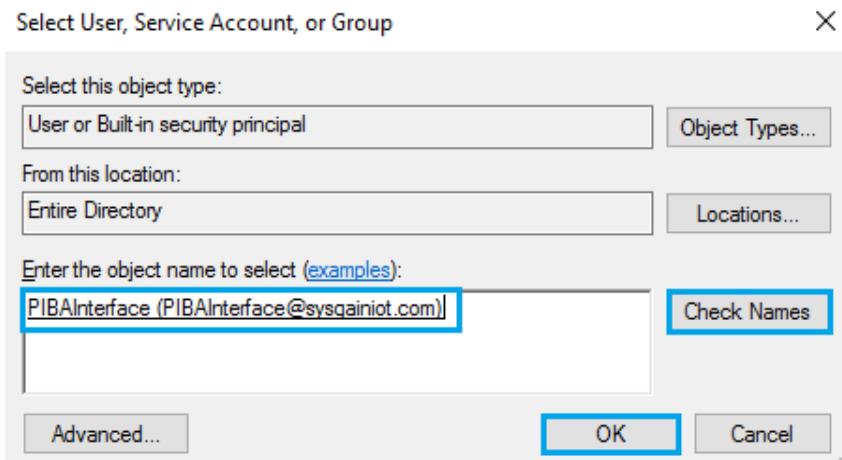
4. Click on **Locations**. You will get a popup box of credentials: enter the SQL server credentials.



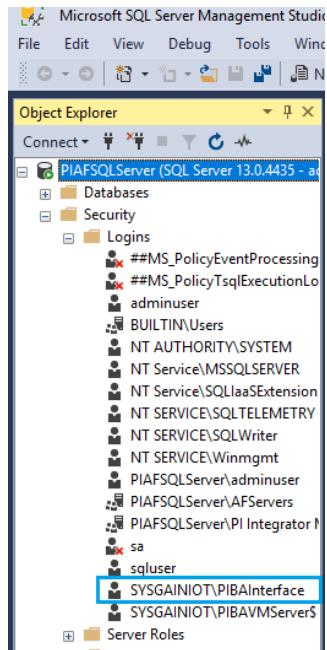
5. Select the **Entire Directory** and click on **OK**.



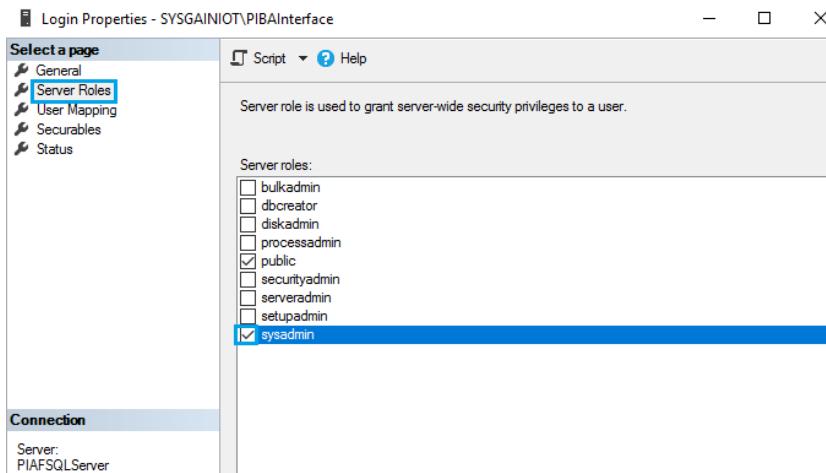
6. Enter the object name as **PIBAInterface** and click on **Check Names**. Then click on **OK**



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

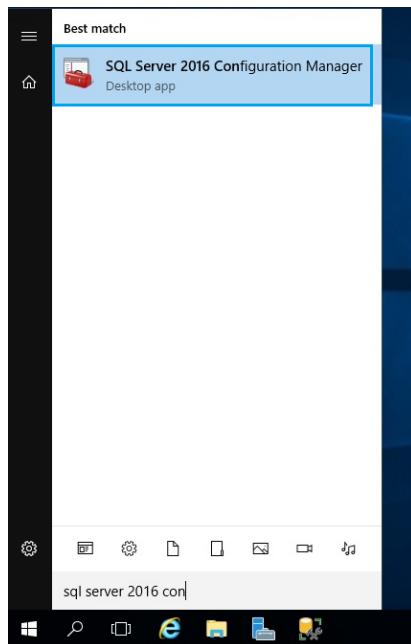


8. Right click on **User (created)** > Right click and select **properties** > click **Server Roles** > check the **sysadmin** box to give permission to the new user.

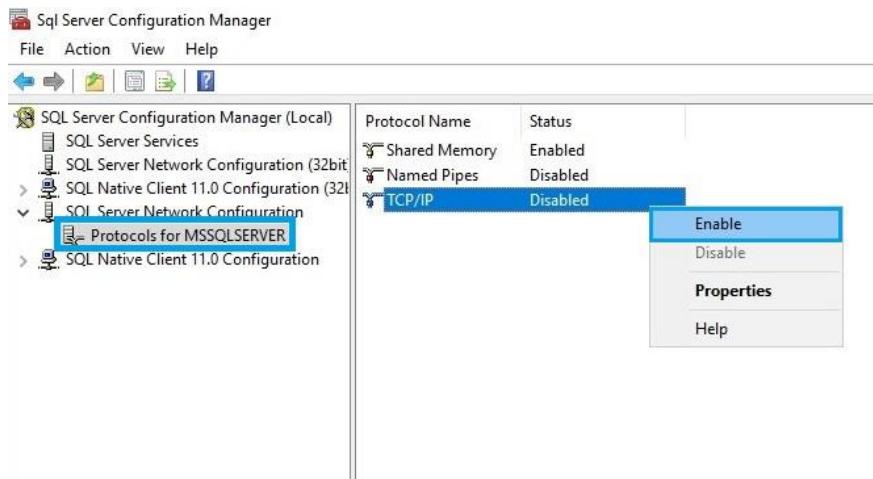


## 8.2. Enable TCP and Named Pipe in SQL Server Configuration Management

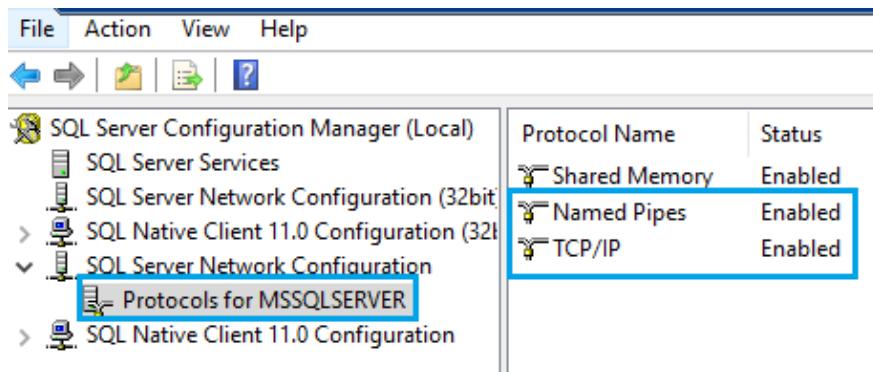
1. From the **Start** menu, navigate to **SQL Server 2016 Configuration Management**.



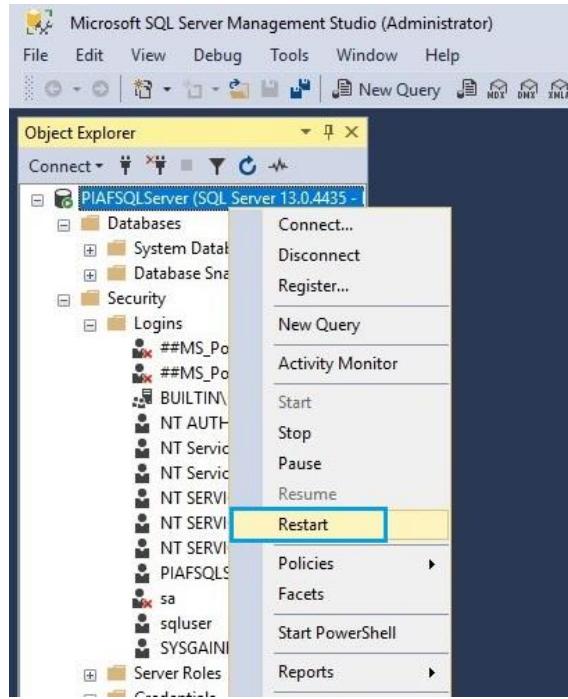
2. Click on **SQL Server Network Configuration > Protocols for MSSQLSERVER**.



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

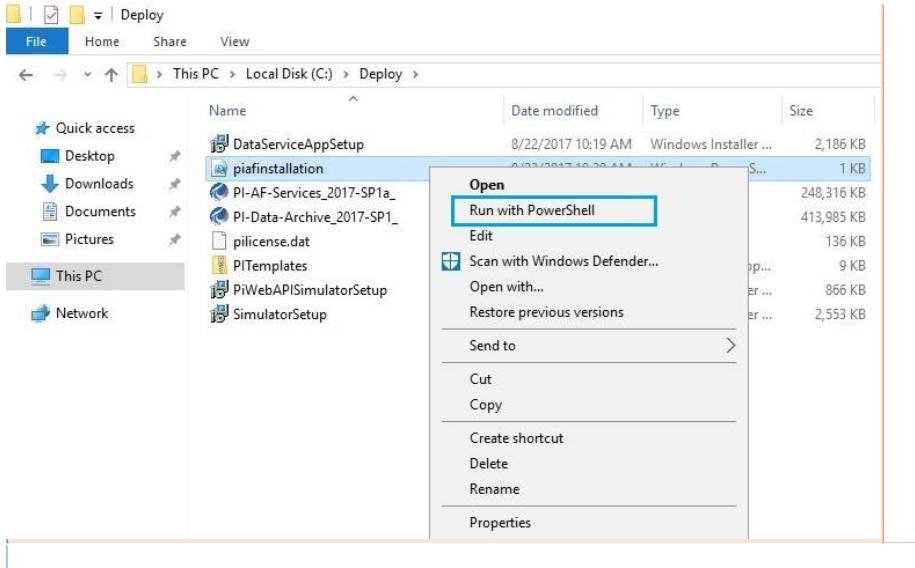
1. Login into **PIAFSQLServer VM** with the Private IP Address from the Bastion Server with the credentials provided in the output section.

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 **admininuser** and **Password@1234** values to update them with your username and password from the PIAFSQLServer and then **save**. After that, right click on the piafinstallation > select **Run with Powershell**.

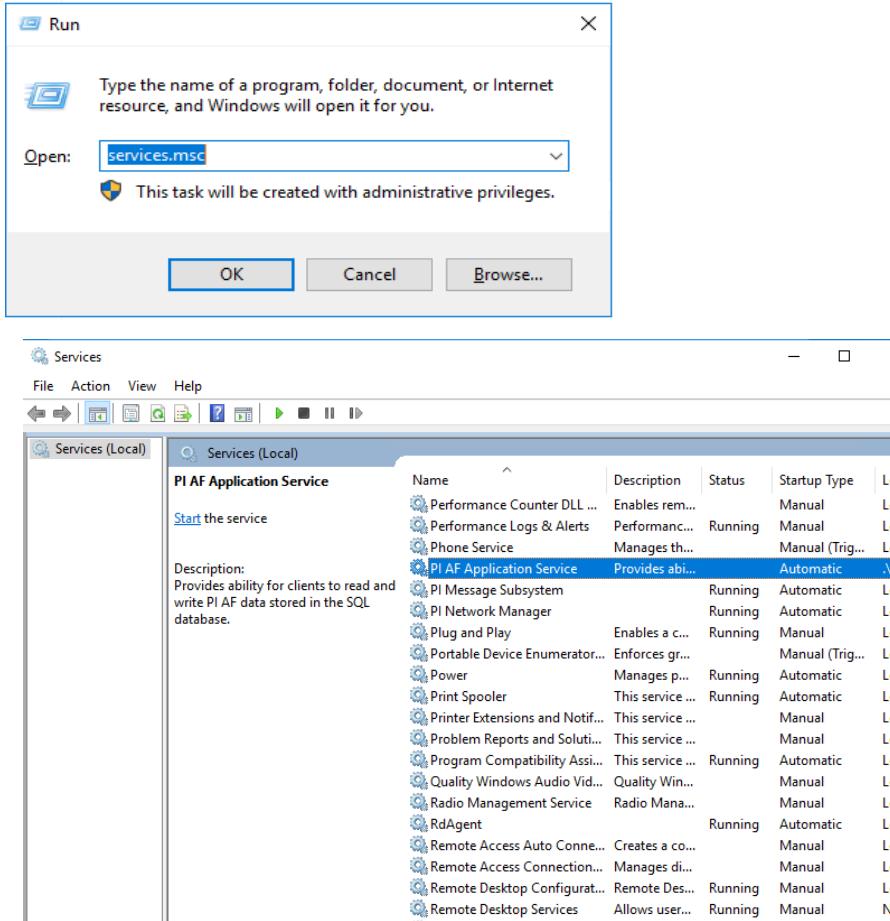
```
C:\Deploy\PI-AF-Services_2017-SP1a_.exe ADDLOCAL=ALL AFSERVICEACCOUNT=PIAFSQLSERVER\adminduser AFSERVICEPASSWORD=Password@1234 FDSQLDBSERVER=PIAFSQLSERVER /quiet
```



Commented [AS37]: Password is hardcoded in this script

Commented [UD38R37]: But in the above step aren't you changing that??

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.

**Commented [MK39]:** There is no PI AF Application Service in services.

**Commented [KO40R39]:** You should be check in PIAFsqserver services. And we forgot to mention that we hardcoded the PISQLServer username ,password in piaf installation powershell script you need to open and change the username password in script then only it is run.

**Commented [UD41R39]:** Komali did you update that now in the document???

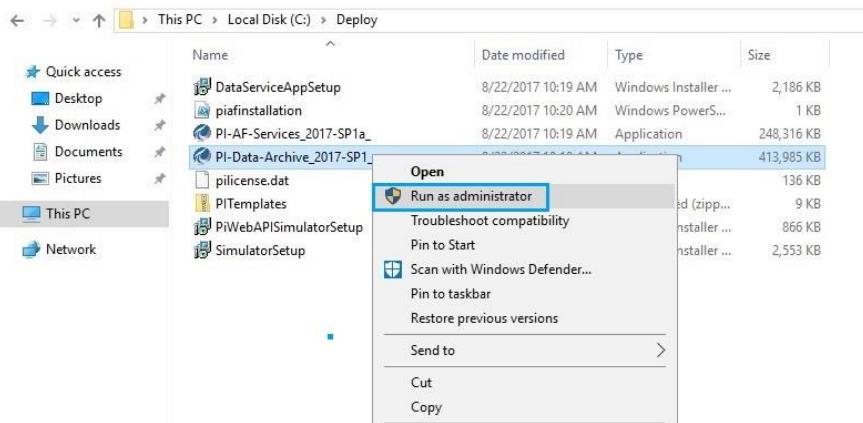
**Commented [KO42R39]:** before i updated when i reply to mohmmed comment

The image shows the 'Services' control panel with a list of services. The 'PI AF Application Service' is missing from the list, which is why the comment above it was made.

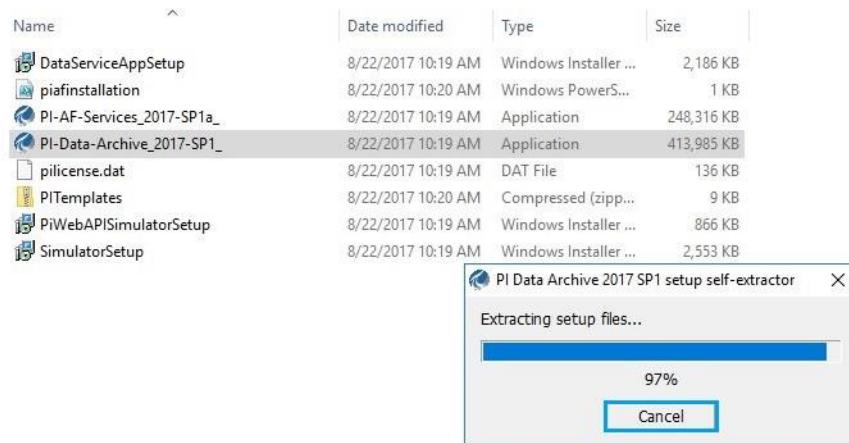
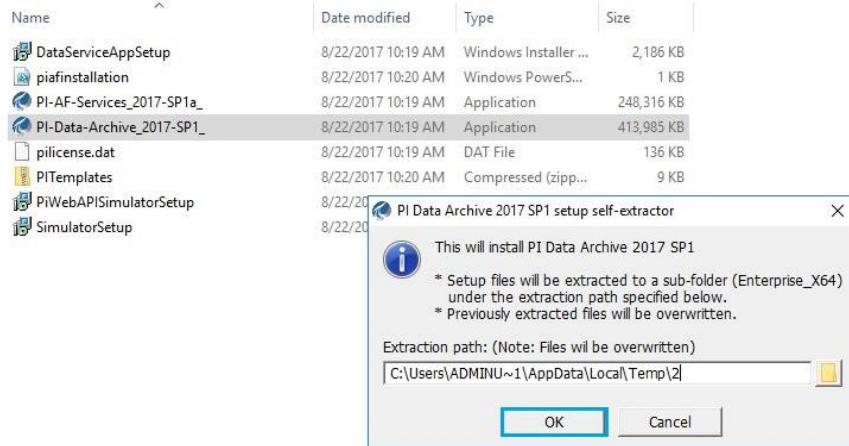
The PI Data Archive collects, stores, and organizes data from data sources, providing an information infrastructure. The PI Server also includes tools for analytics, alerts, and auditing. The PI Server may be connected to almost any existing automation, lab, or information system. Operators, engineers,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

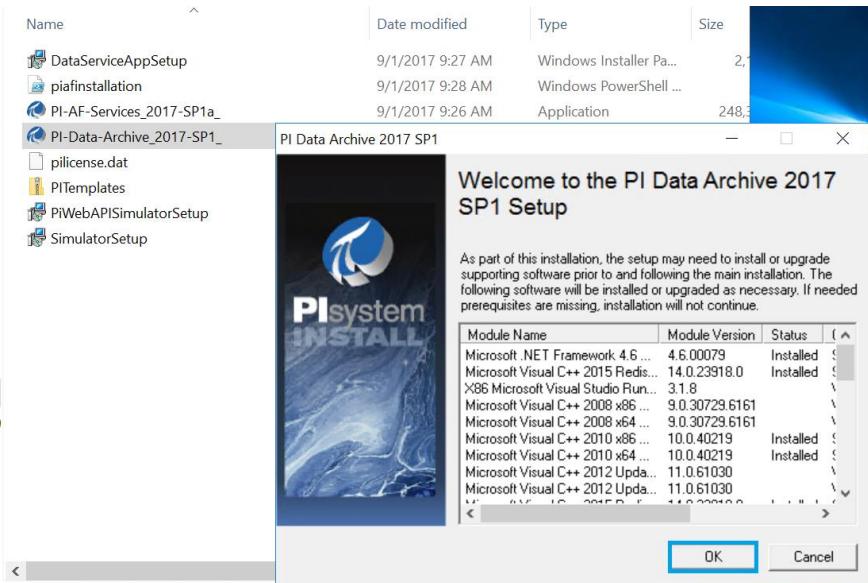
1. Navigate to **Local disk (C:)** > **Deploy** > select **PI-Data-archive\_2017-SP1** > right click and **Run as administrator**.



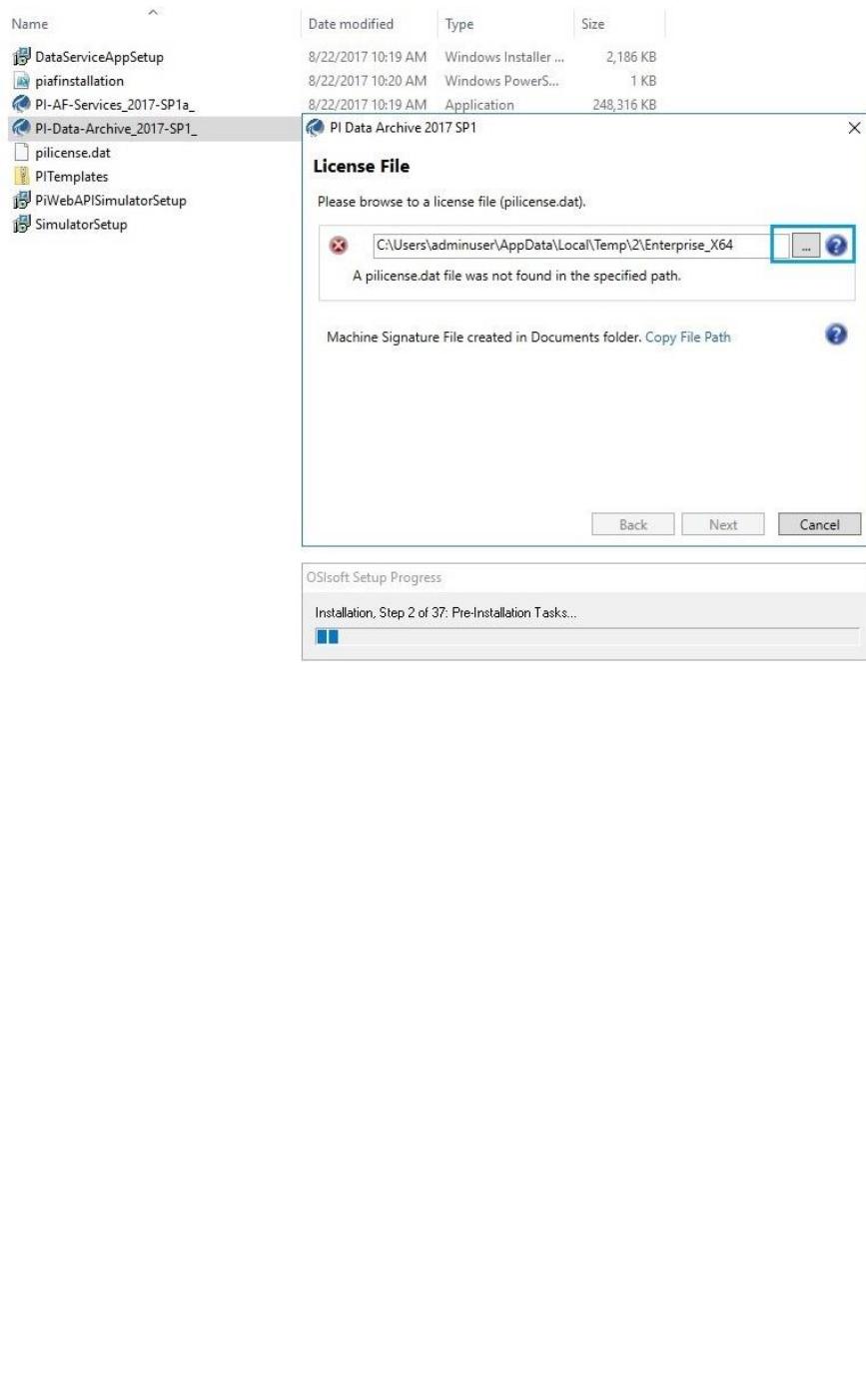
2. Click on **OK**.



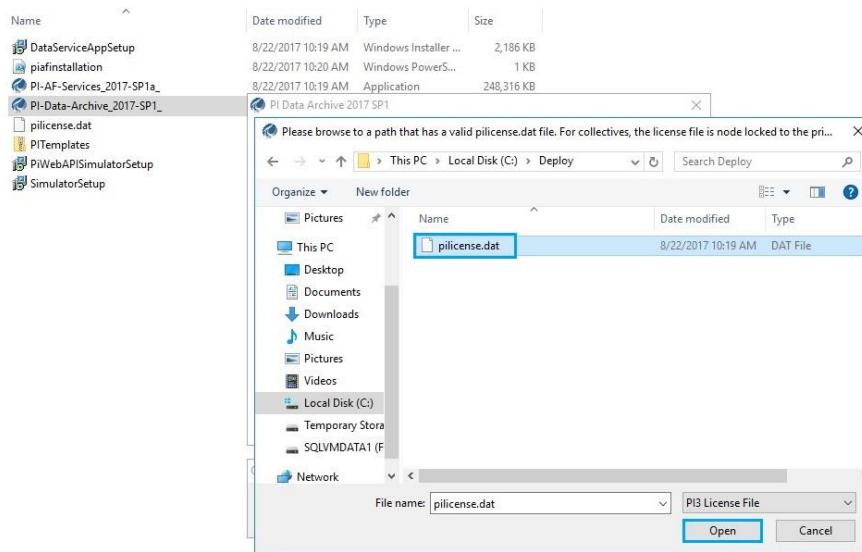
3. Click on **OK**.



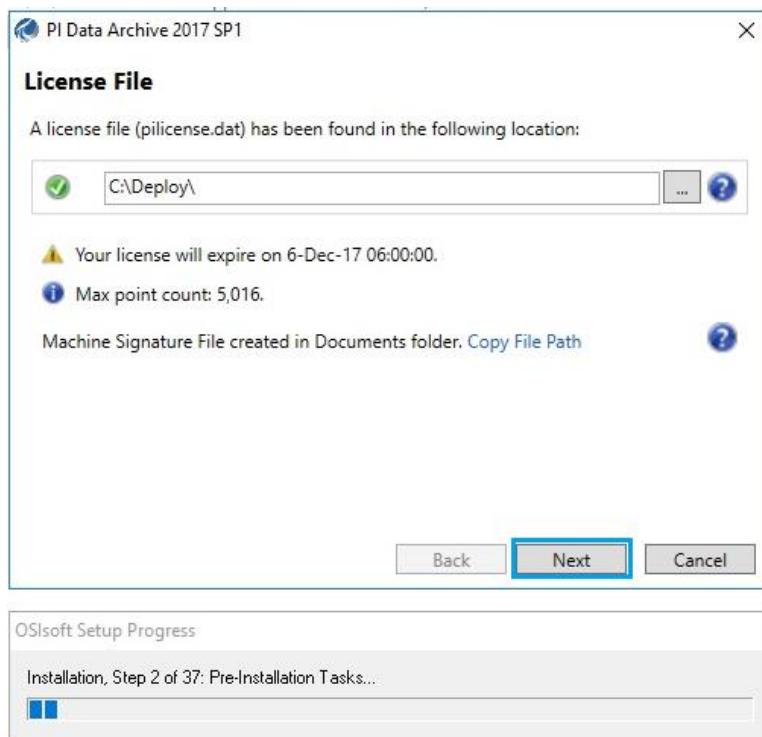
4. After completion of extracting setup files, click on **OK**.



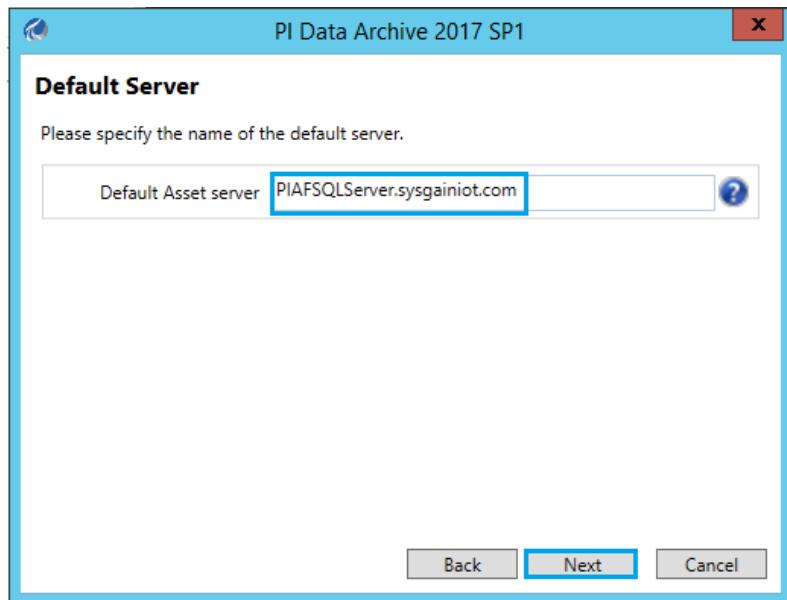
5. Click on the browse option, then navigate to the **Local disk (C:)** > **Deploy** > select **pilicense.dat** and click on **Open**.



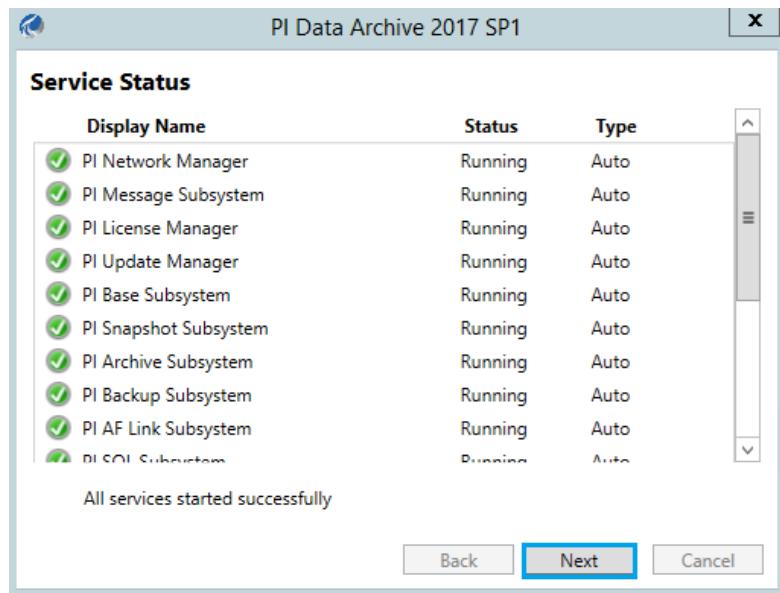
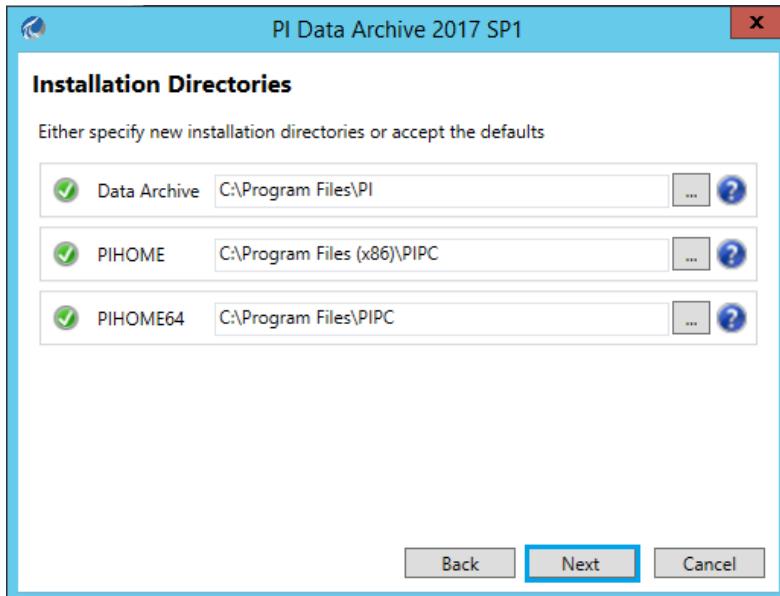
6. After that, click on **Next**.



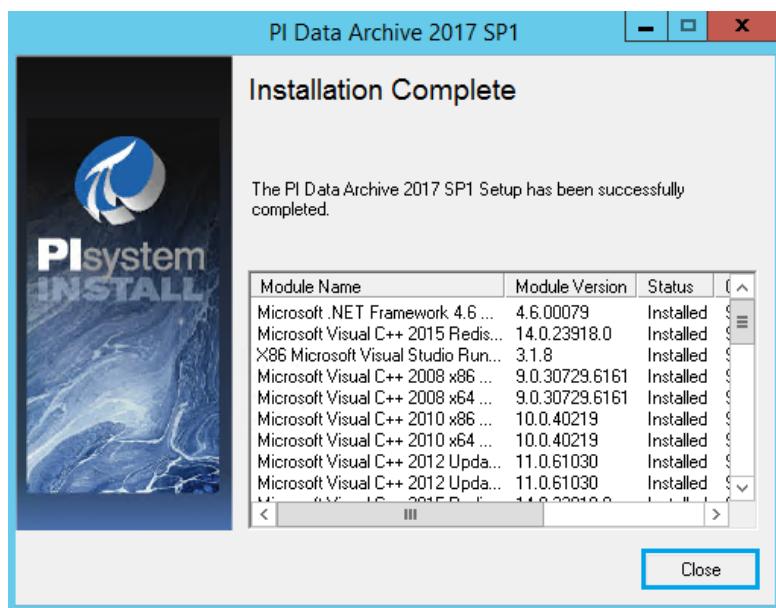
7. Add the domain name to the **Default Asset server** and click on **Next**.



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

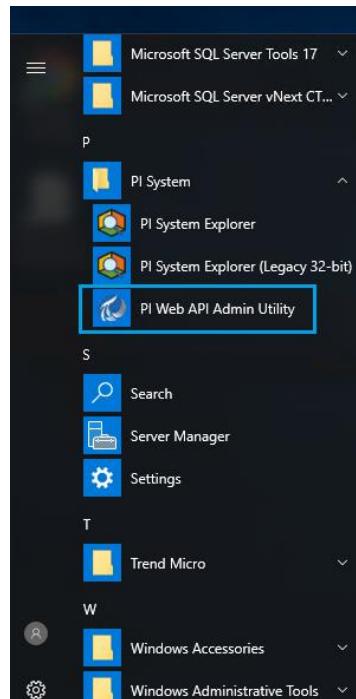


9. Click on **Close** once the installation is completed.

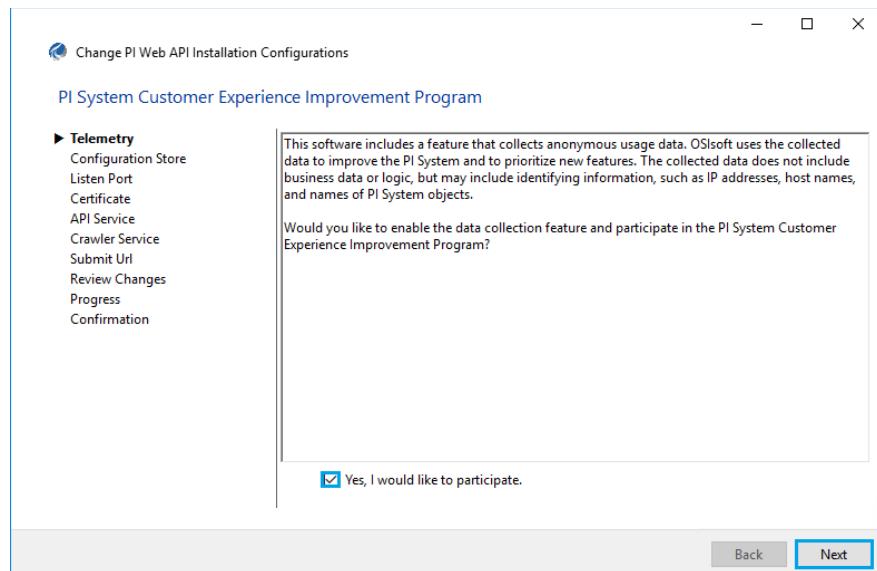


### 9.3. PI Web API Utility

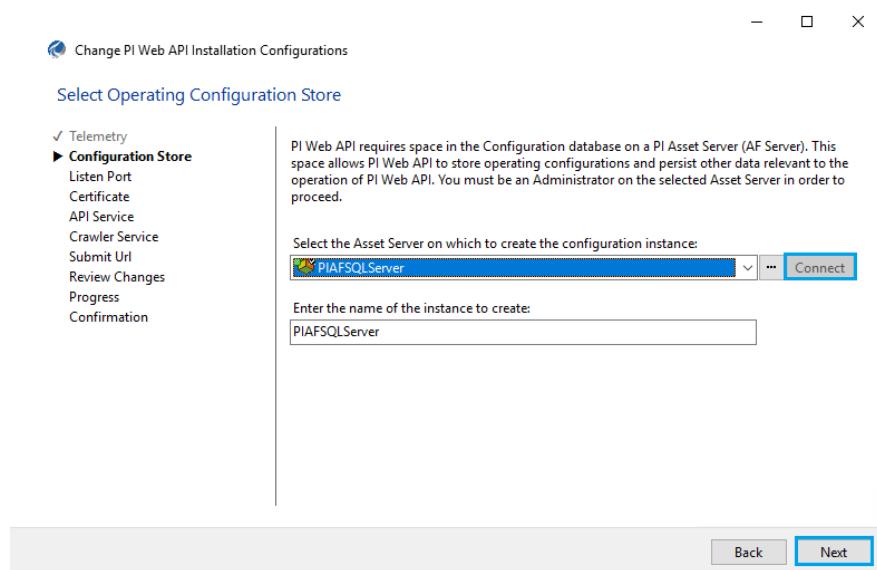
1. Navigate to **PI System > PI Web API Admin Utility** from the Start menu.



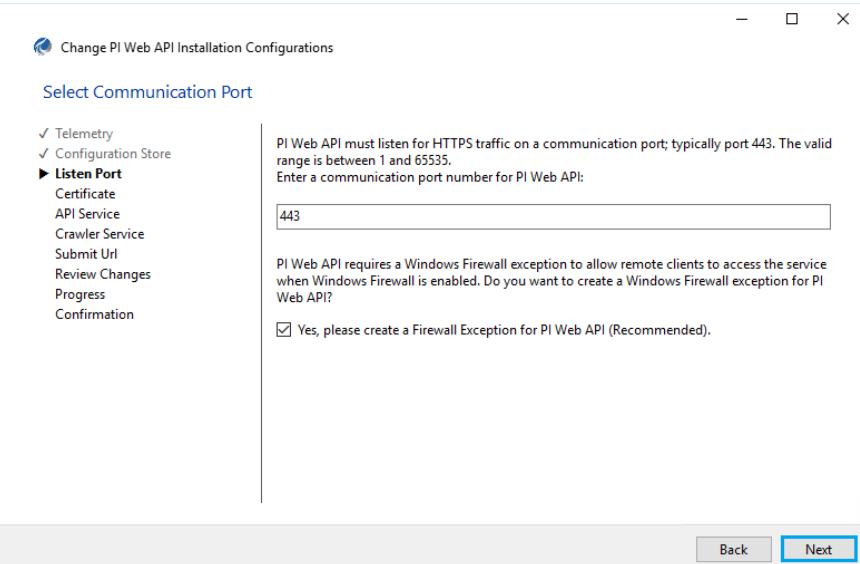
2. Check the **Yes, I would like to participate** dialog box and click on **Next**.



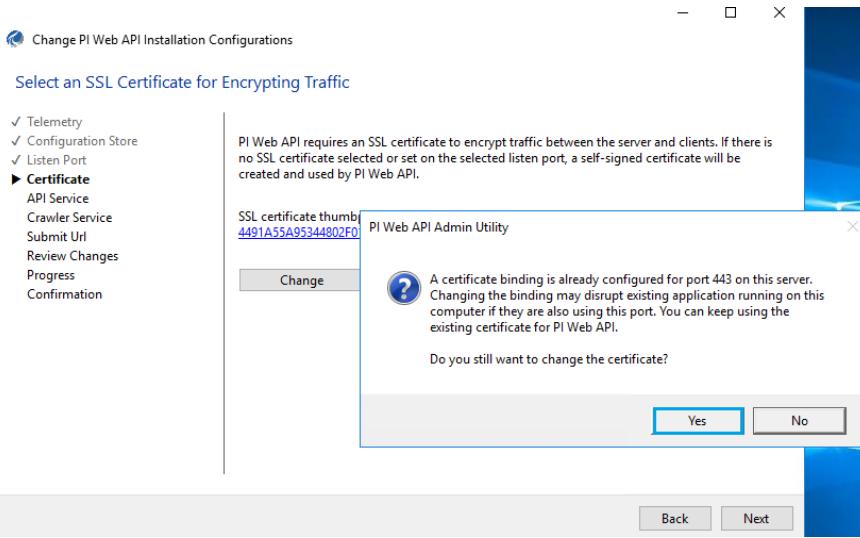
3. Select **Connect** and click on **Next**.



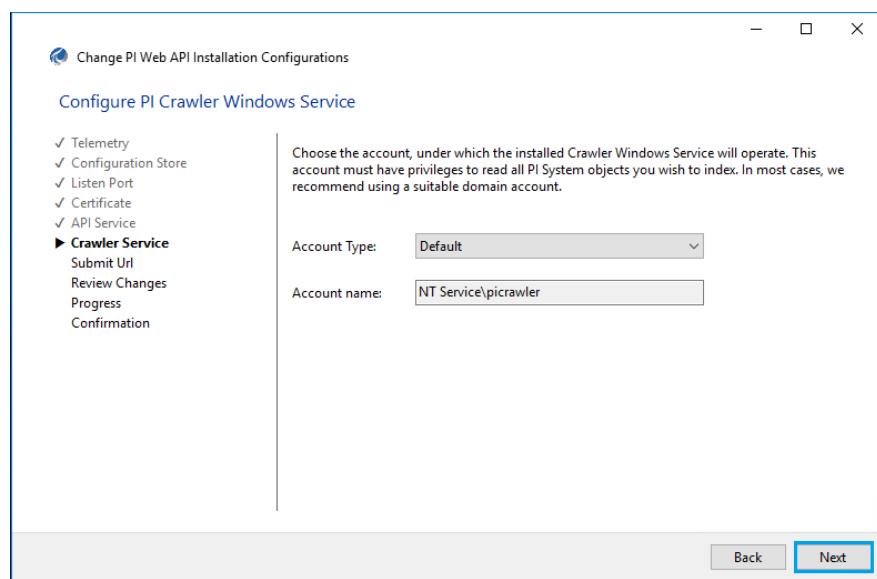
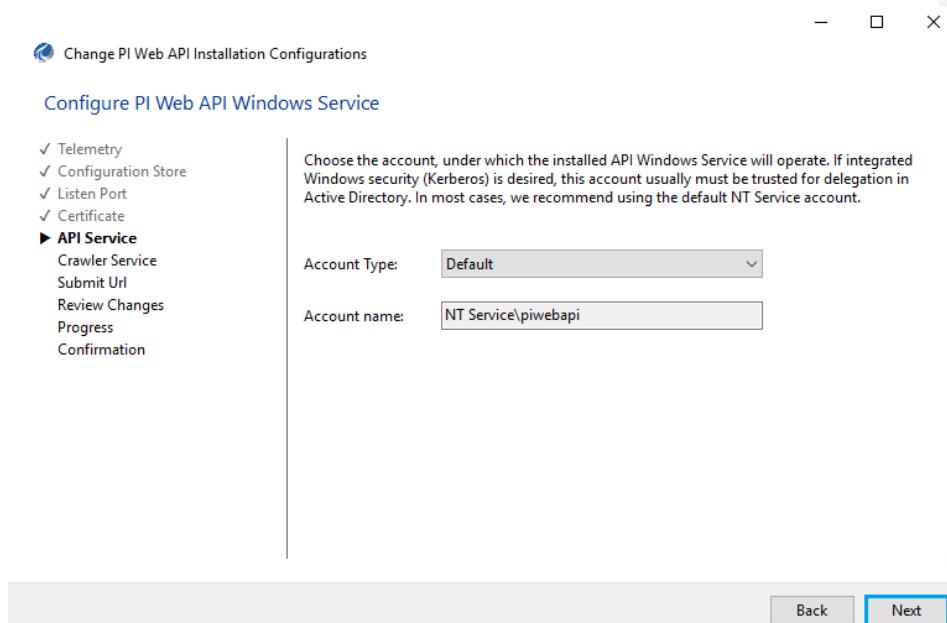
4. Click on **Next**.



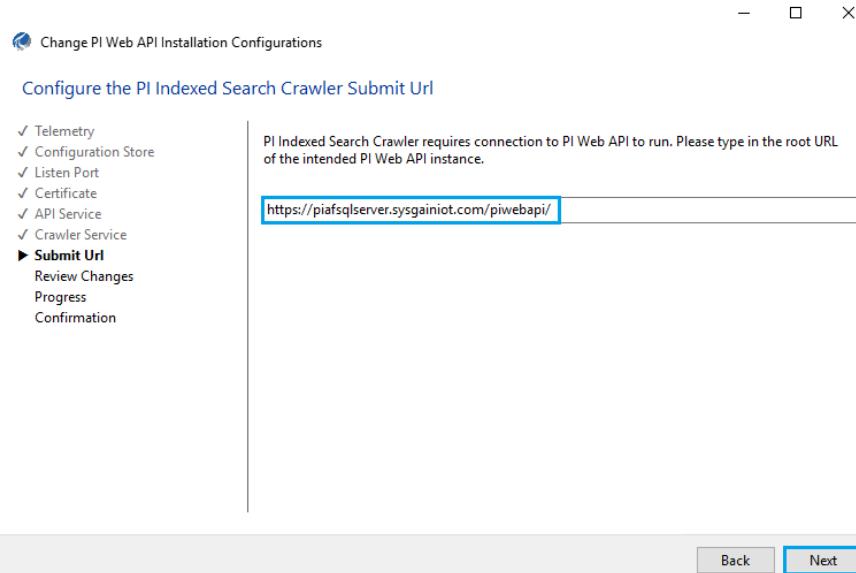
5. Click on **Remove** to remove the certificate and then click on **Yes**.



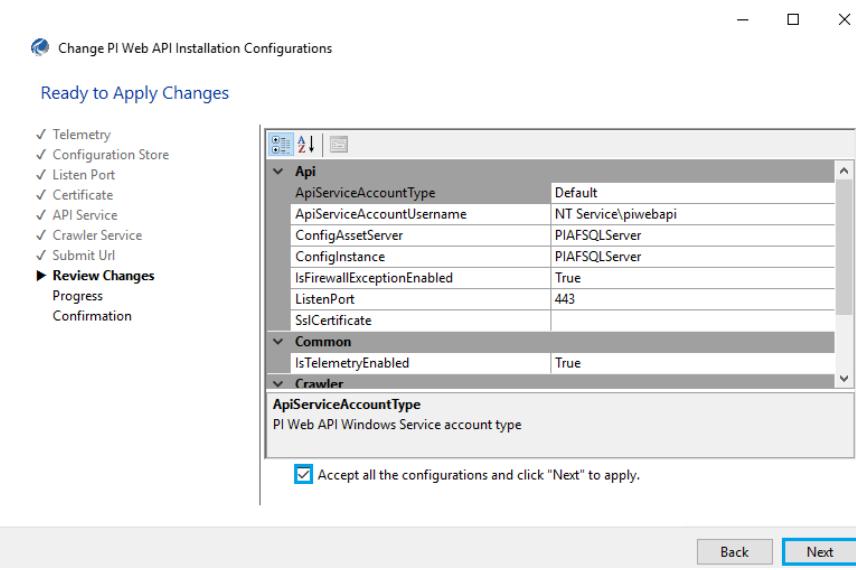
6. Configure **API Service** and **Crawler service** and click **Next**.

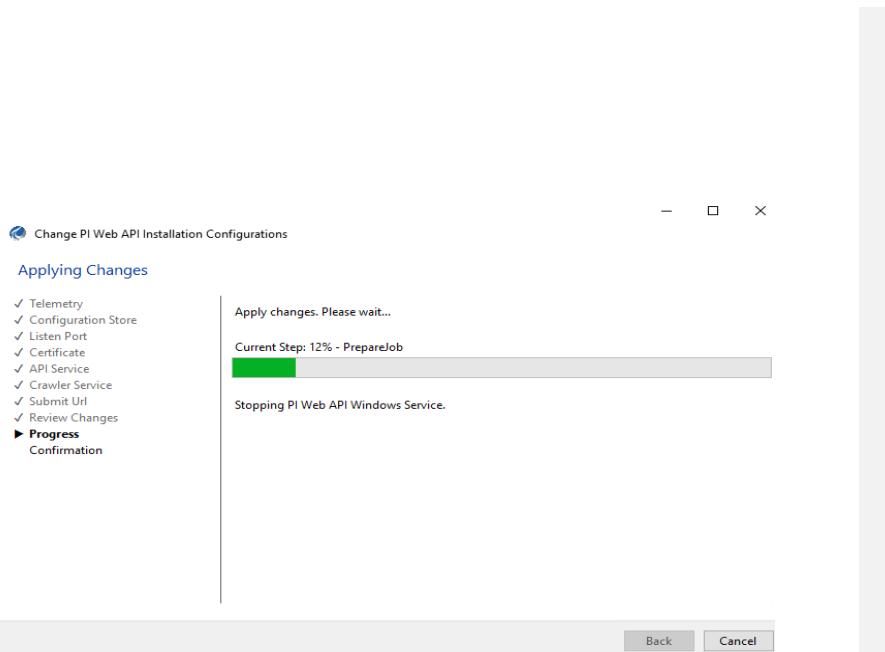


7. Note down the **Submit URL**.

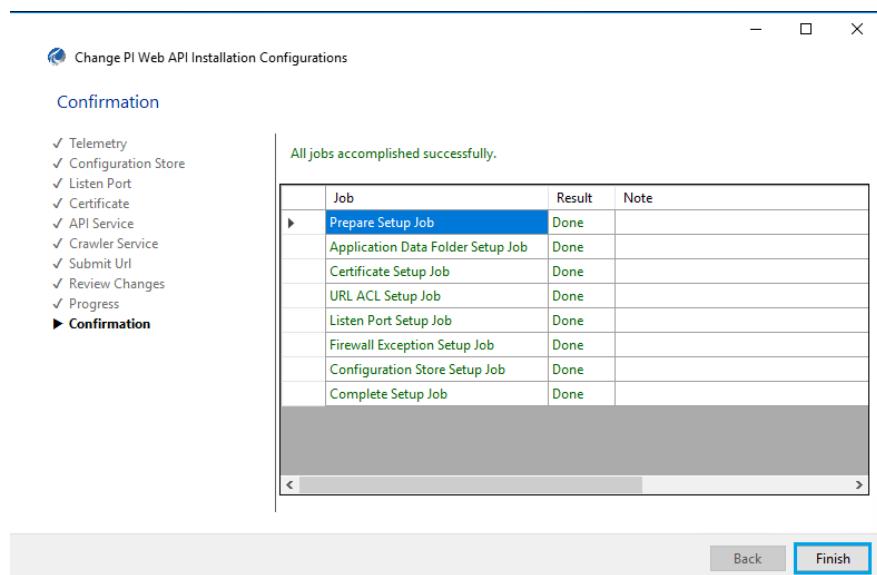


8. Check **Accept all the configurations** and click on **Next**.



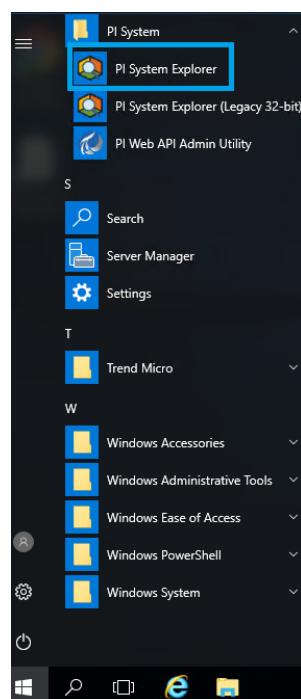


9. Click on **Finish**.

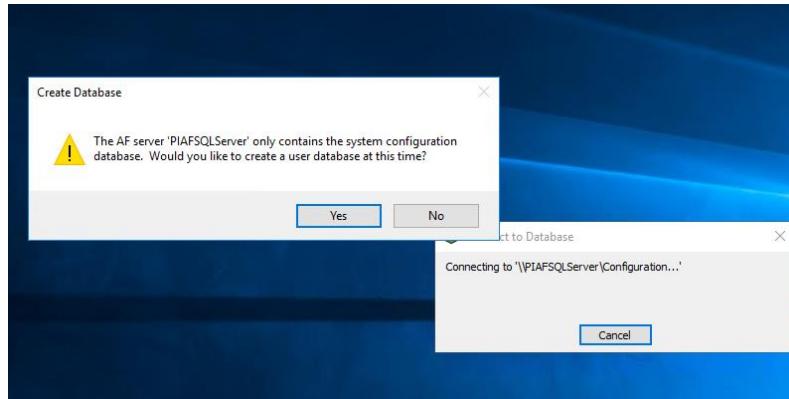


## 9.4. Creation of Database in PI System Explorer

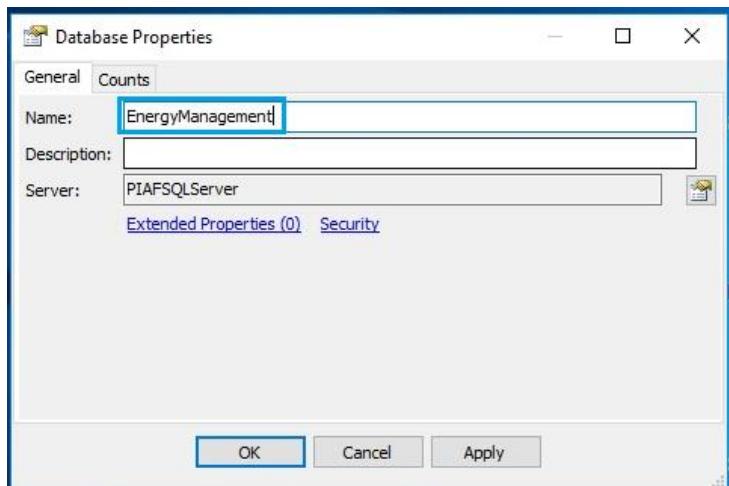
18. On the PIAFSQL machine, Navigate to **PI System Explorer** in PI System folder from the Start menu.



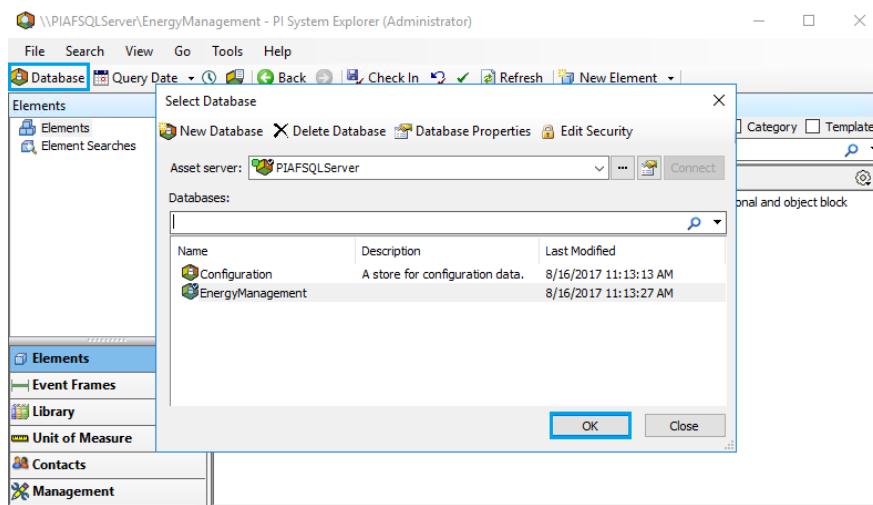
19. Two popups show up, **Connect to Database** and **Create Database**. Click **Yes** on the **Create Database** popup.



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

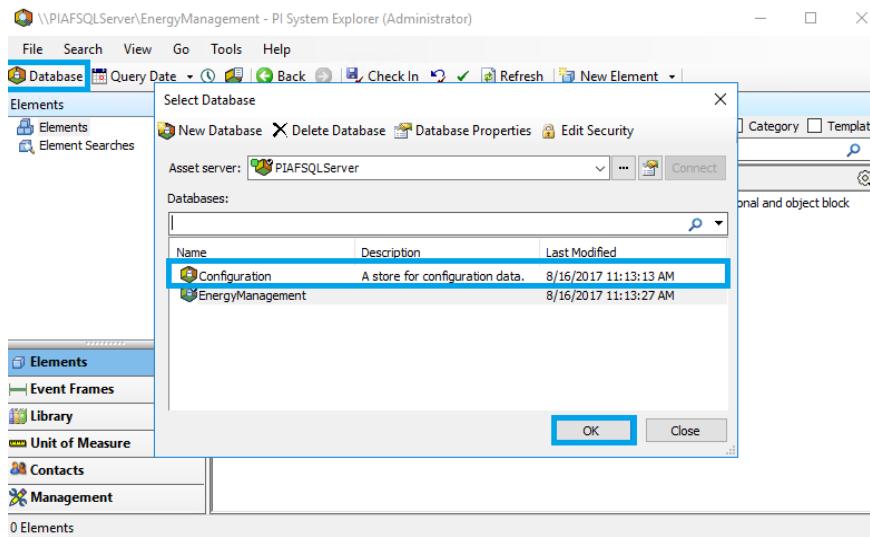


21. Navigate to **PI System Explorer**, click on **Database** to view the created database and click on **OK**.

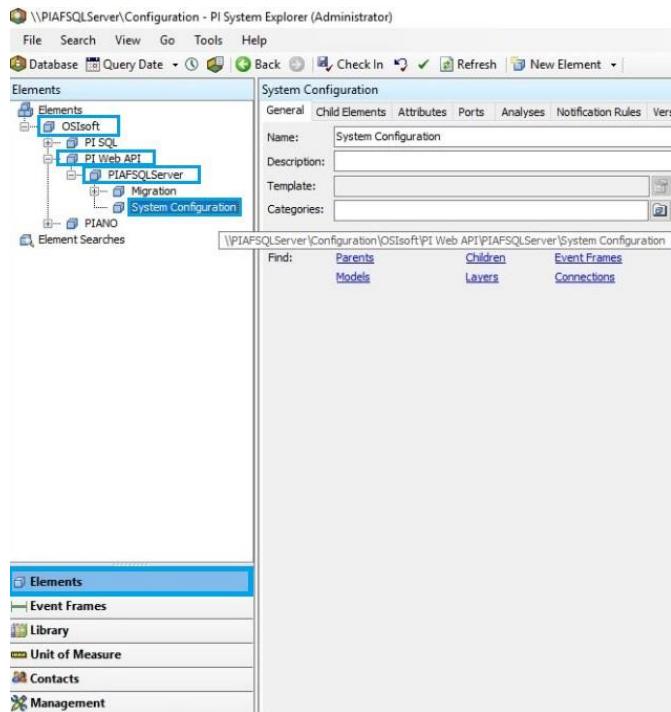


## 9.5. System Configuration in PI System Explorer

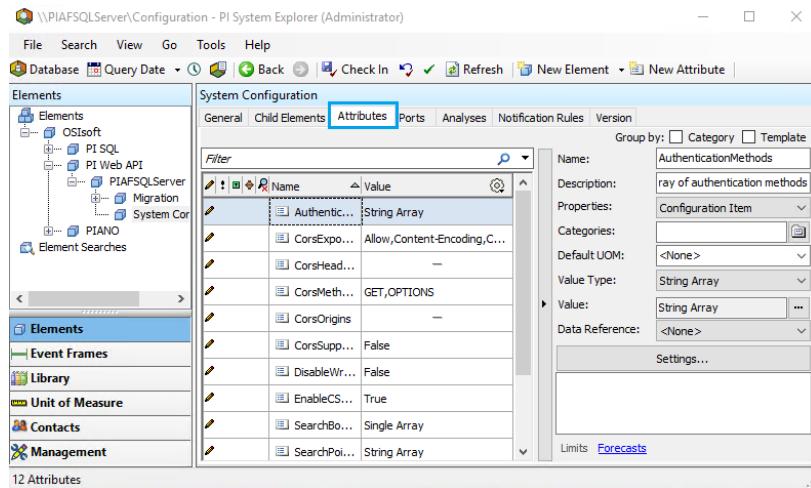
1. Navigate to **PI System Explorer** > Click on **Database** > click **Configuration** under Databases section. Click **OK**.



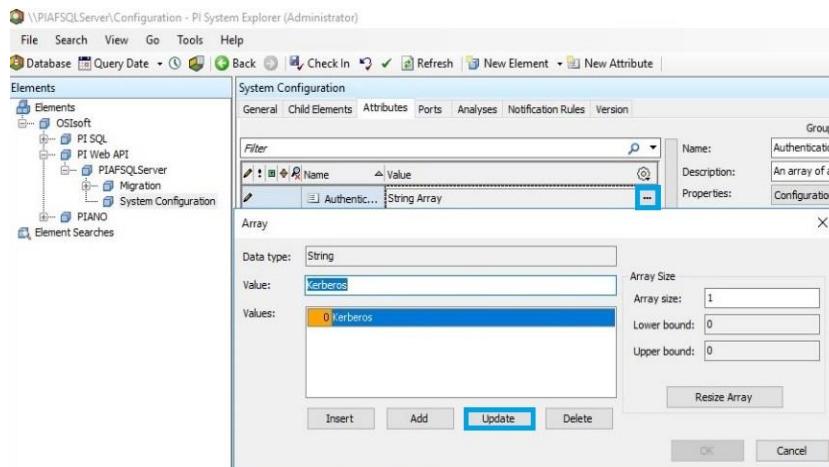
2. Click on **Elements** and navigate to **OSISoft > PI Web API > PIAFSQLServer > System Configuration.**



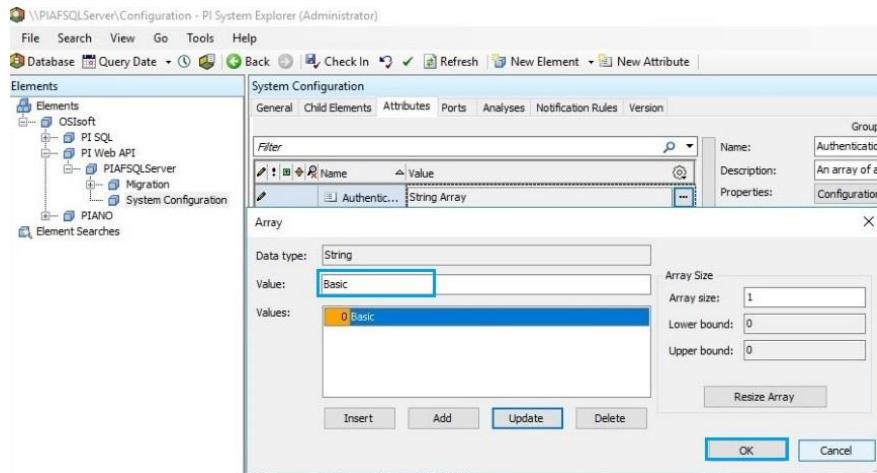
3. Click on **Attributes**.



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

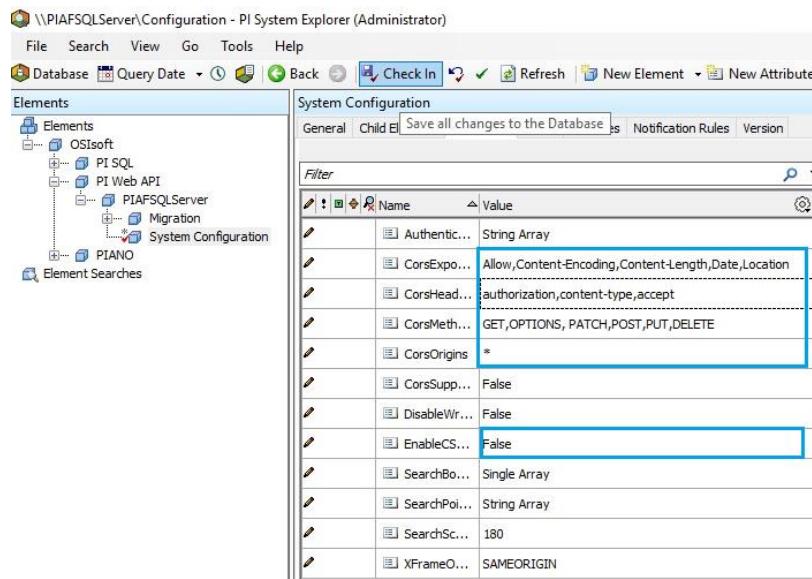


5. Click on **Update**, then **OK**.

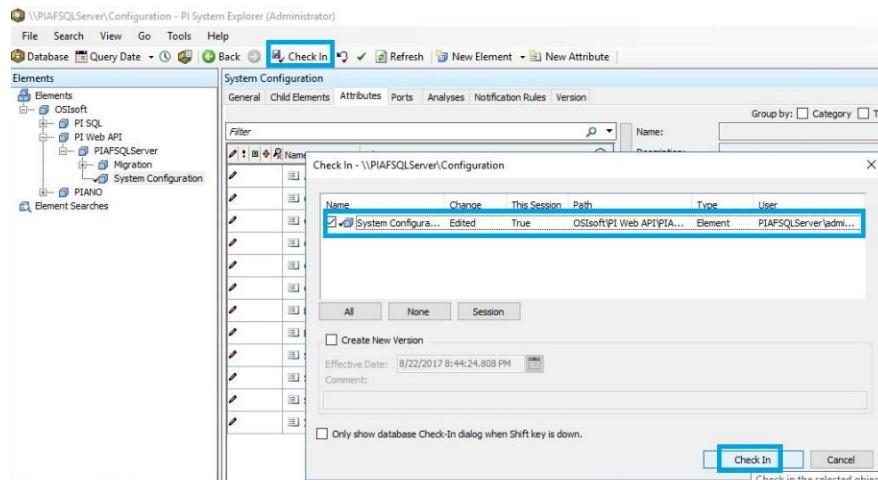


6. Similarly, change the following values:

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

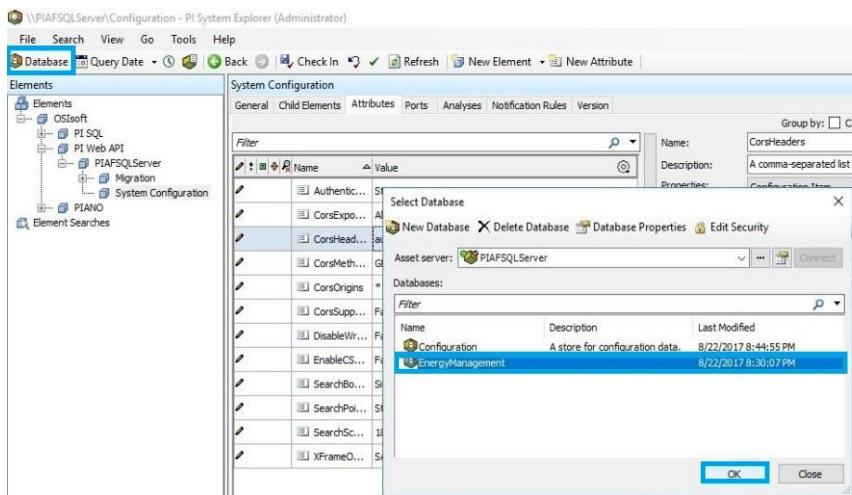


7. Select the **System Configuration** again and click on **Check In**.

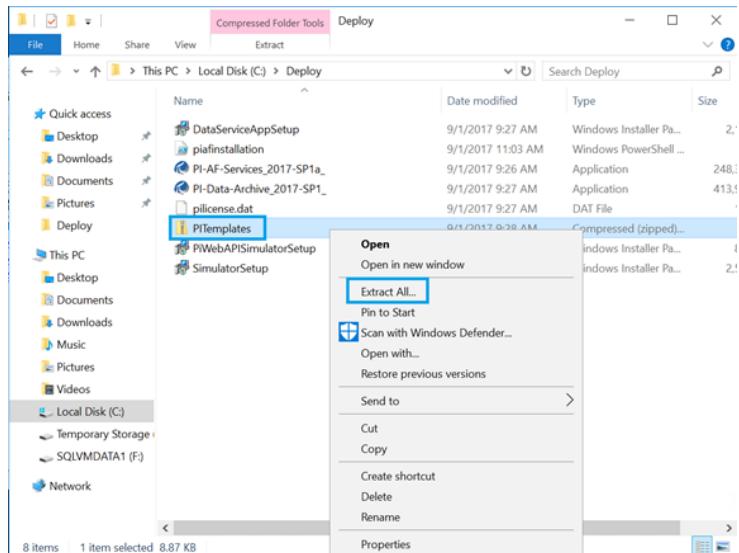


## 9.6. Import .XML Files into AF Server

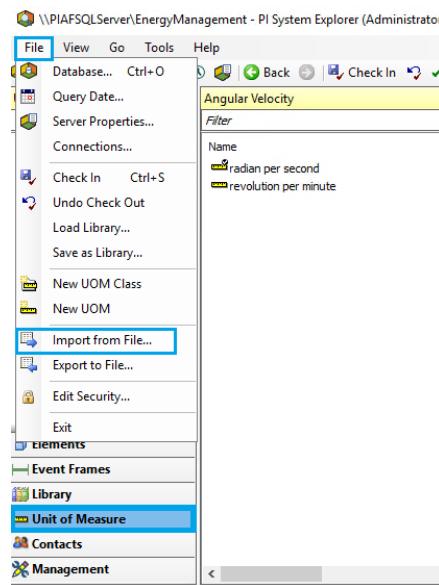
1. From the Bastion host connect to the **PIAFSQLServer** virtual machine through the private address with the credentials provided in the output section.
2. Navigate to **PI System Explorer > Select Database > Click on Energy Management > Click on OK.**



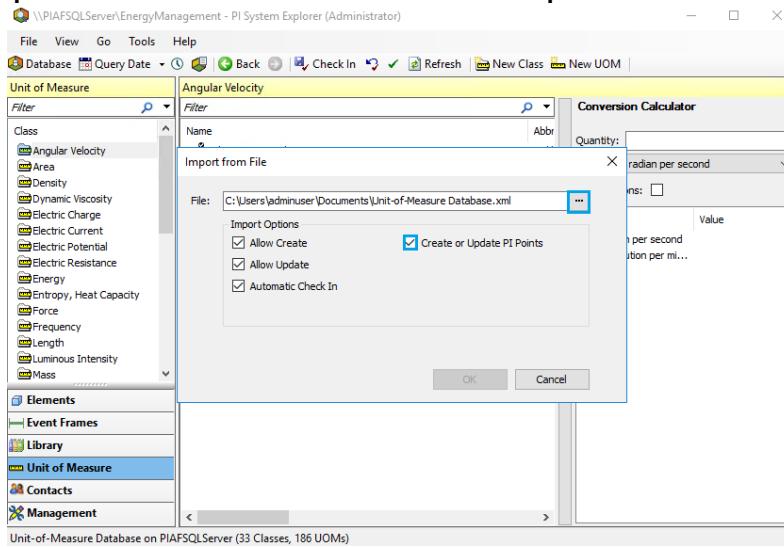
3. Navigate to **Local disk (C:) > Deploy > unzip PI templates.**



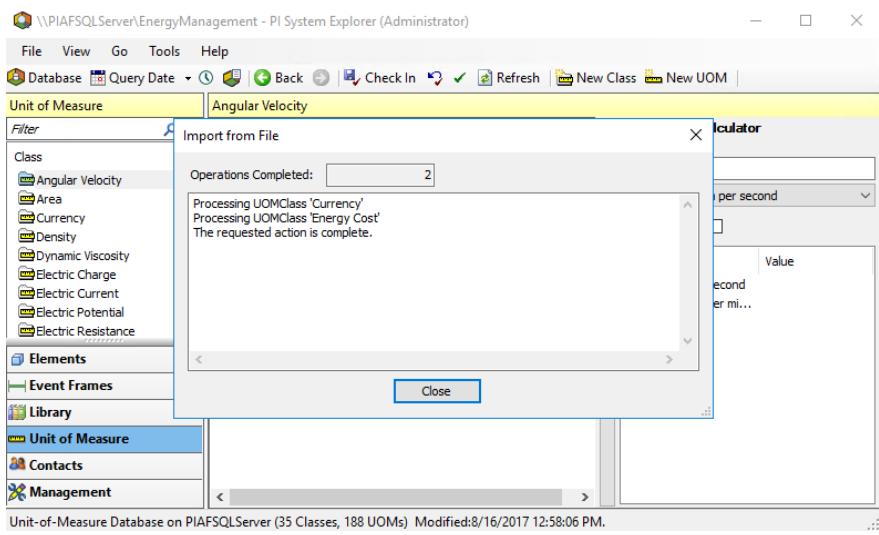
4. Select **Unit of Measure > File > Import from file**



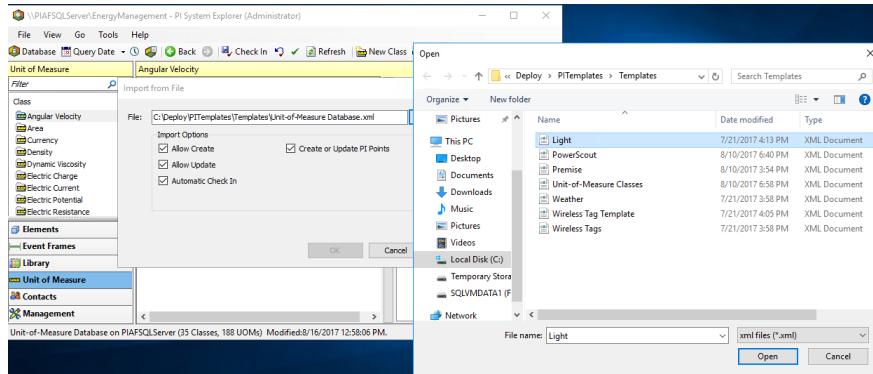
5. Check the box for **Create or Update the PI Points** > browse to local disk (C:) > Deploy > PIITemplates > Select **Unit of Measure Classes** > Click on **Open**.



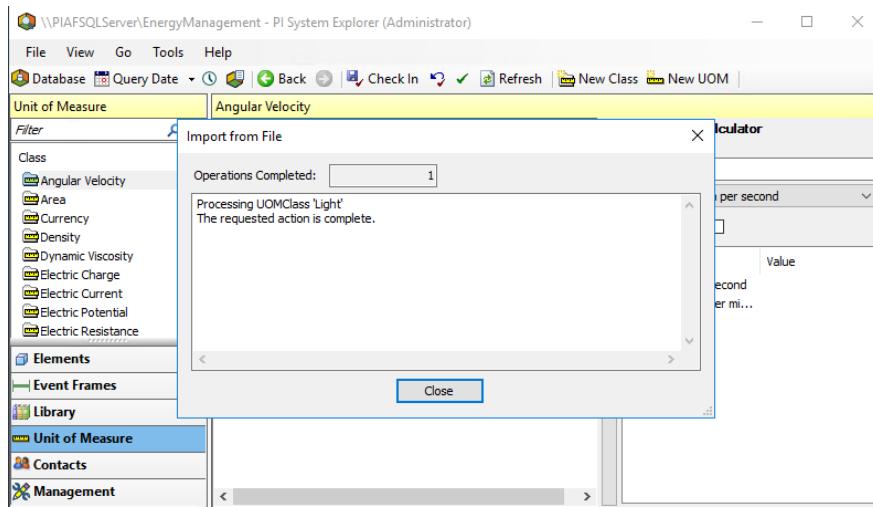
6. You can find the status of the completed operation. Click on **Close**.



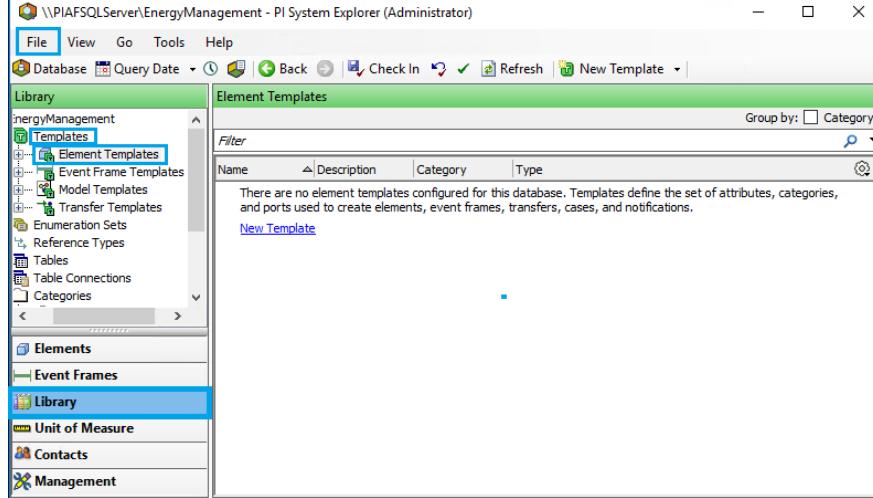
7. Check the box **Create or Update the PI Points** > browse to **C:\Deploy\PITemplates** > Select **Light** and click on **Open**.



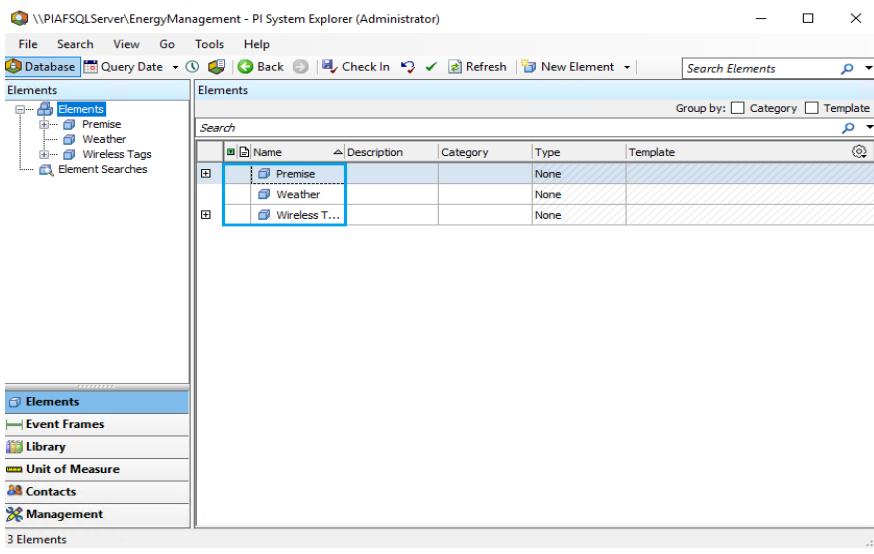
8. You can see the status of the completed operations. Click on **Close**.



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

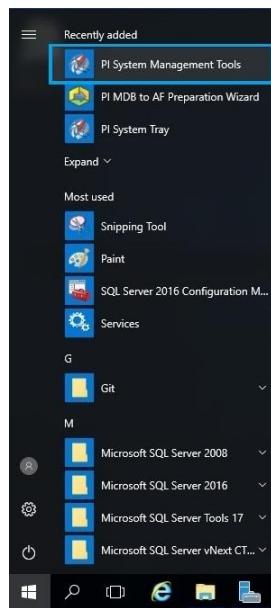


10. Similarly Select **Elements > Import File** (File location – C:\Deploy\PITemplates\Templates).
- Weather
  - Premise
  - Wireless Tags

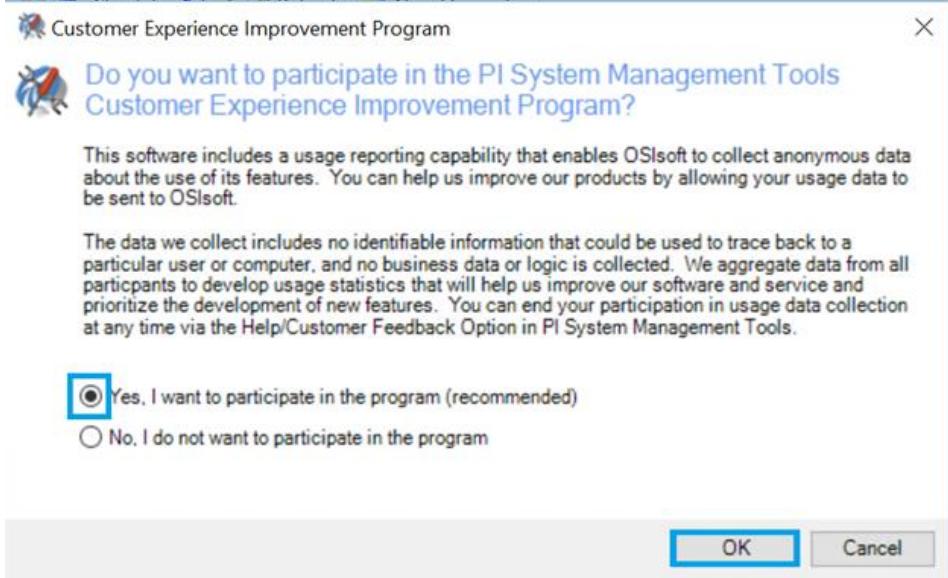


## 9.7. Update Security in PI System Management Tools

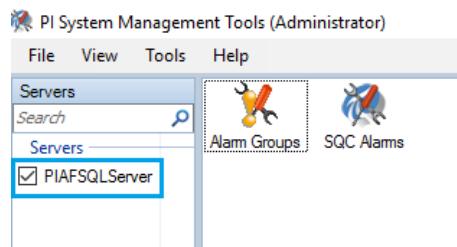
1. From the Start menu, open the **PI System Management Tools**.



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



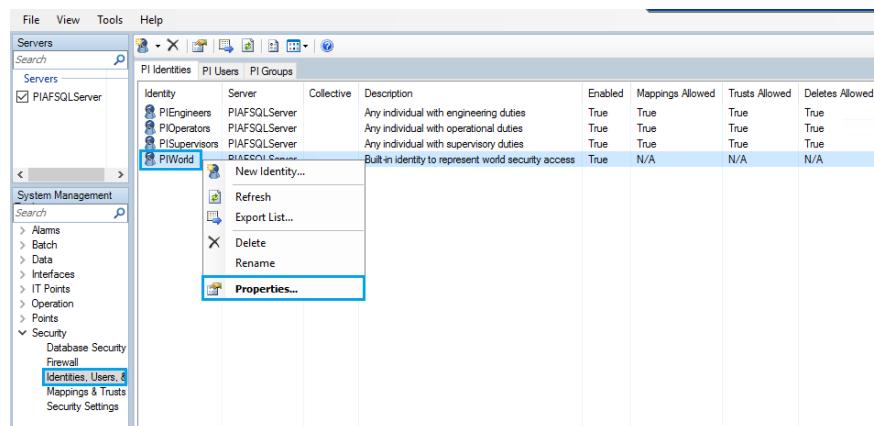
3. Under Servers, check the **PIAFSQLServer** box.



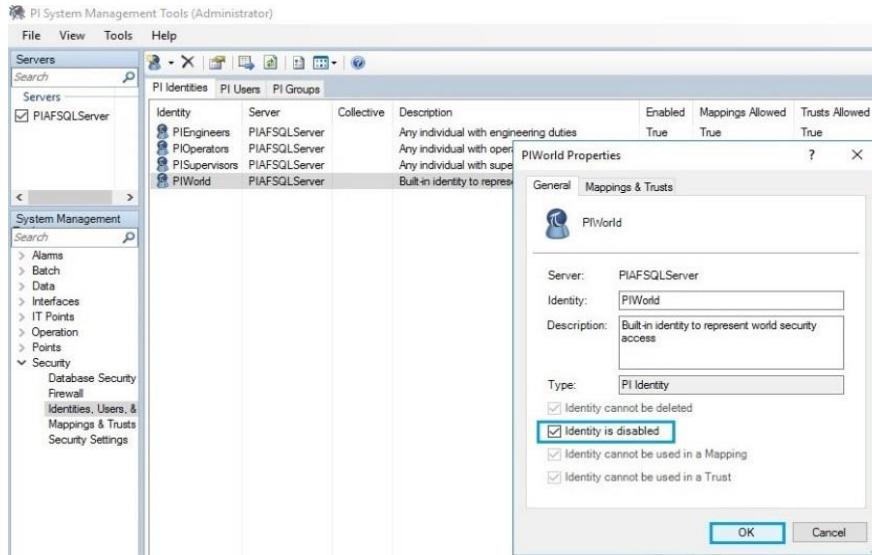
4. Click on **Security** under **System Management**, then click on **Security Settings**.



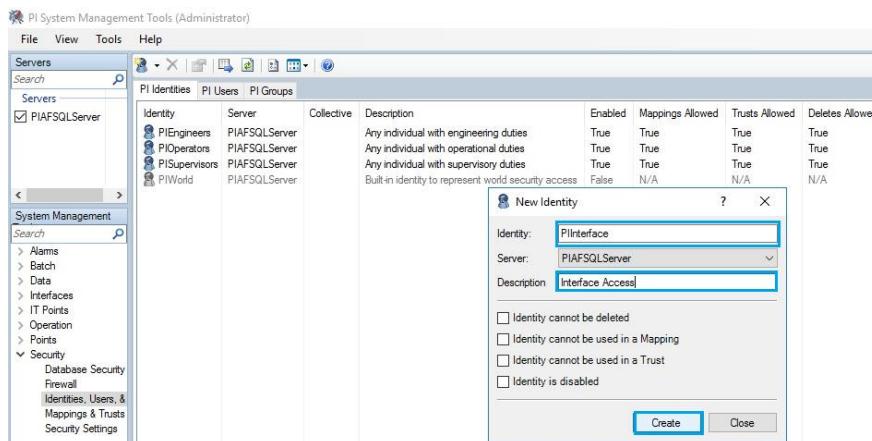
5. Click on **Identities, Users and Groups**, then right-click on **PIWorld** under PI identities and select **Properties**.



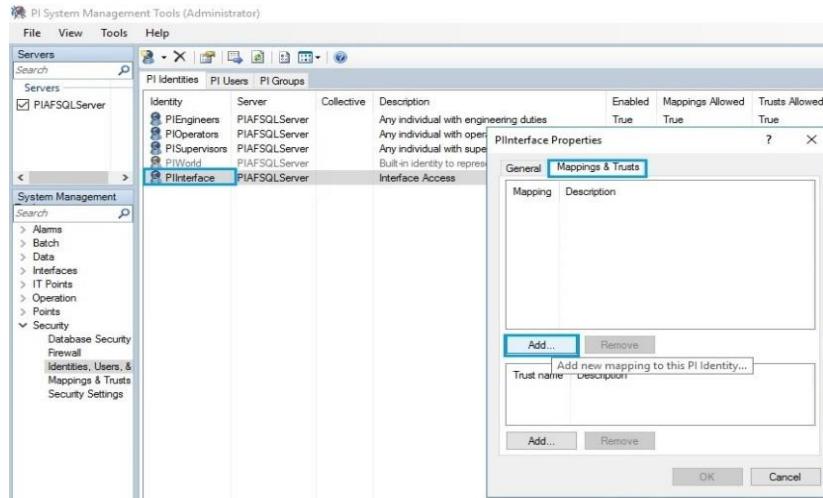
- Select the **Identity is disabled** checkbox and click on **OK**.



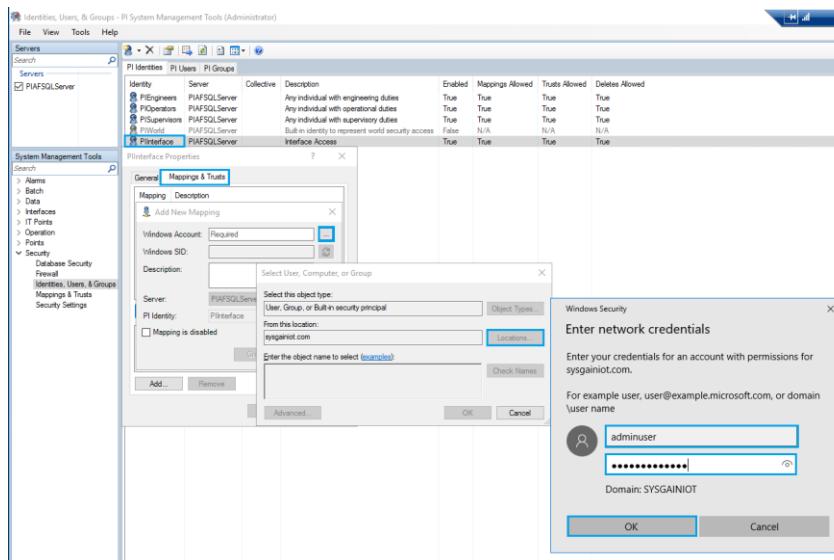
- The **Enabled** column under **PIWorld** will appear as **False**.
- Right-click **PI Identities** to create a new identity. Give the identity the name **PIInterface** and the description **Interface Access**, then click on **Create**.



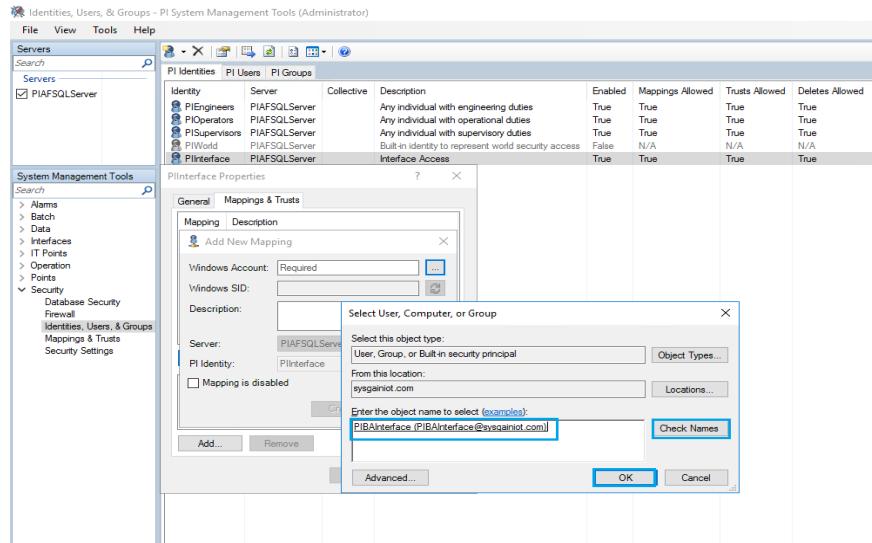
9. Right-click on the newly created **PInterface** identity, then go to **Properties > Mappings & Trusts**, then click on **Add**.



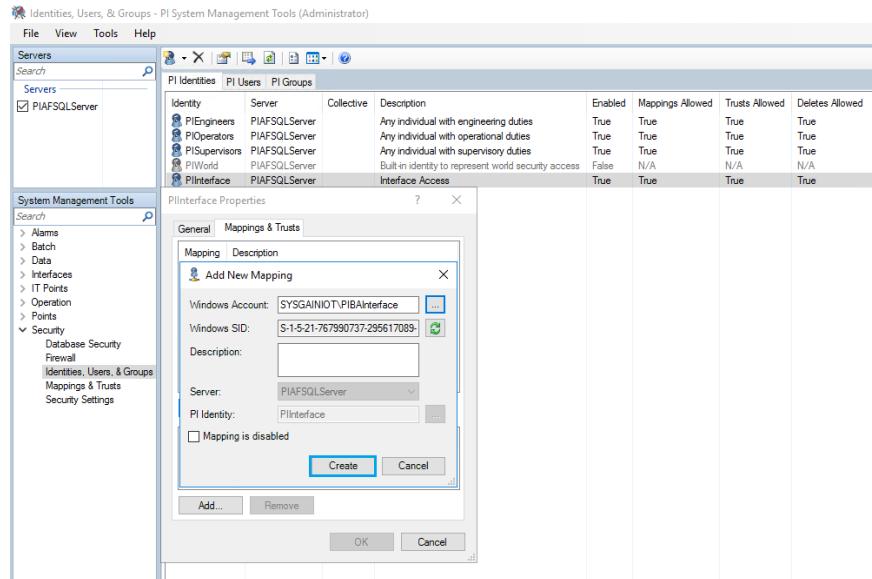
10. After click on **Add** it will show the popup box Add new mapping in that **Browse** at end of **Windows Account** again it will show the popup box as select user,computer,or group in that click on **Locations**. select the domainname Enter the credentials and click on **OK**



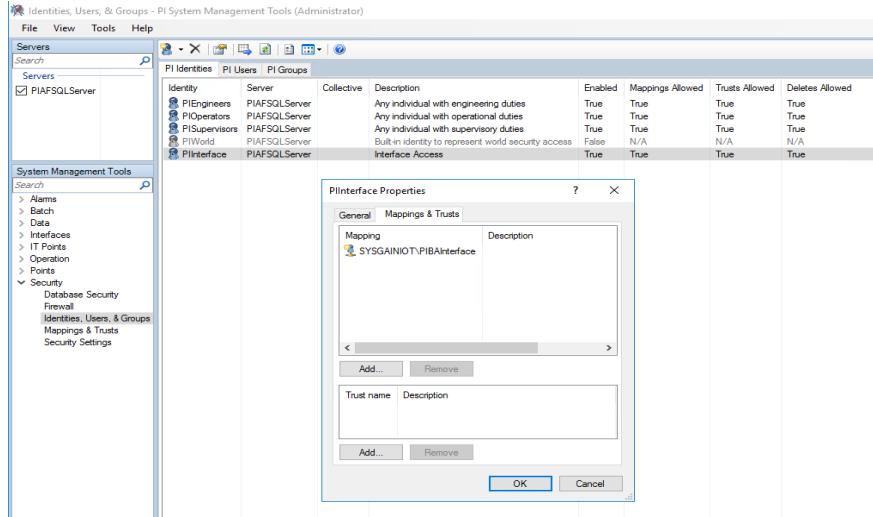
11. Give object name as **PIBAInterface** > Click on **Check Names** > **OK**



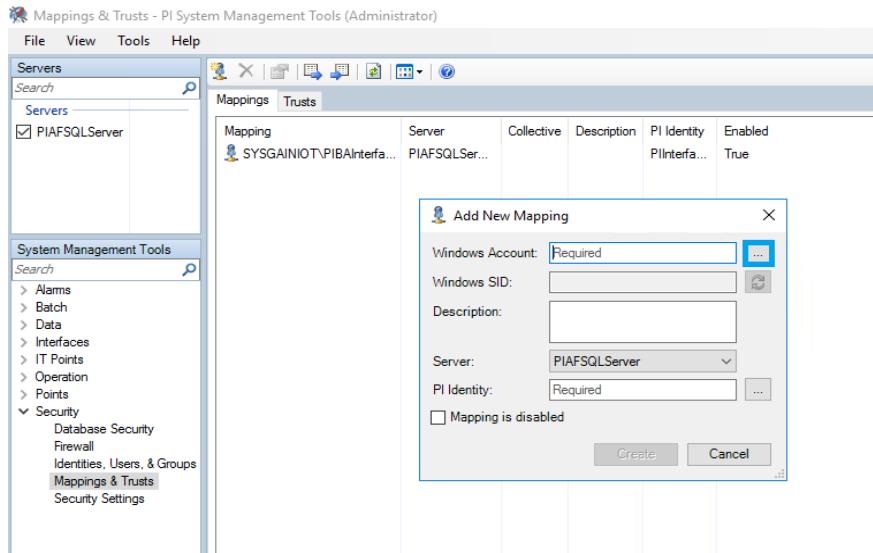
12. Click on **Create** to create a New Mapping for PIBAInterface.



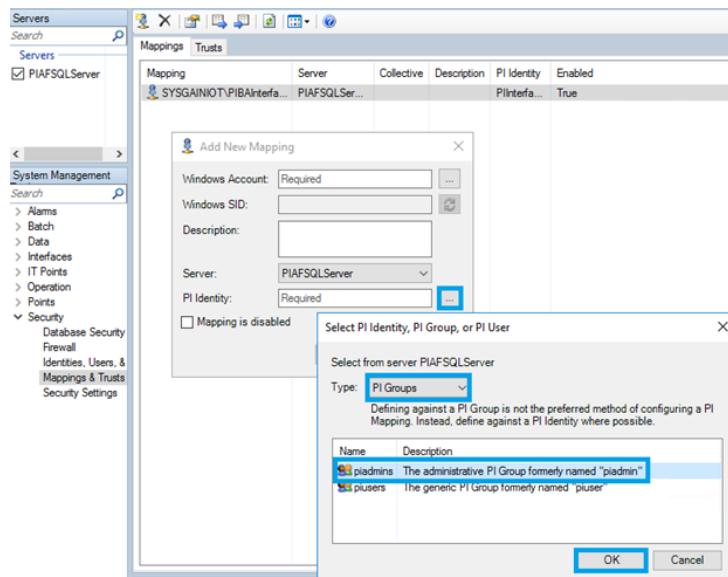
13. Click **OK** once the PIBAInterface mapping is created.



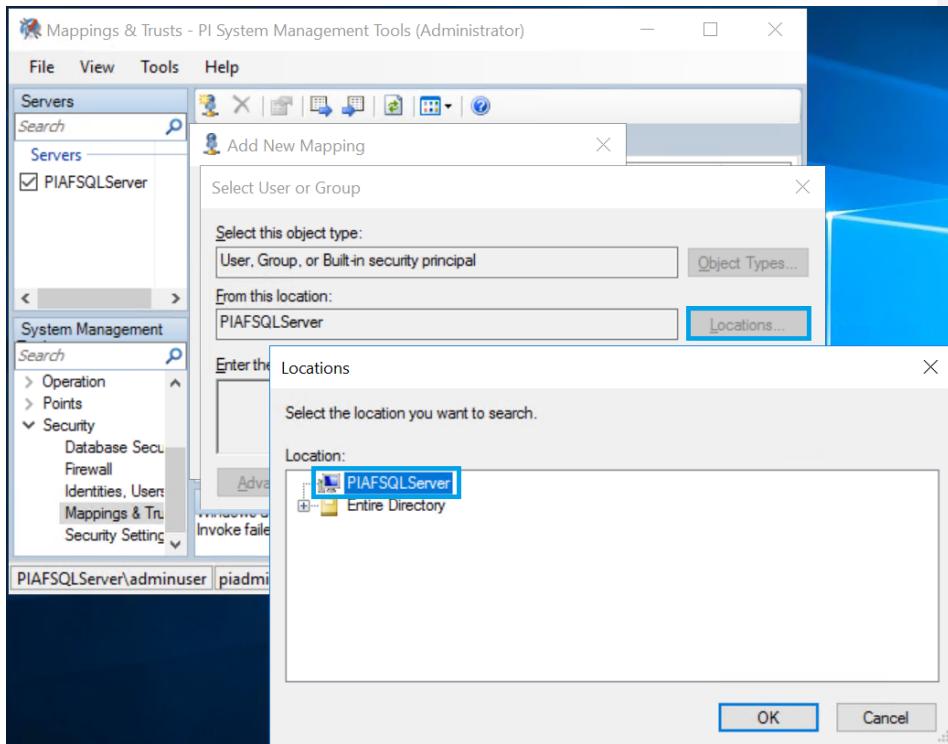
14. Navigate to **Security > Mapping & Trusts** to create a New Mapping.



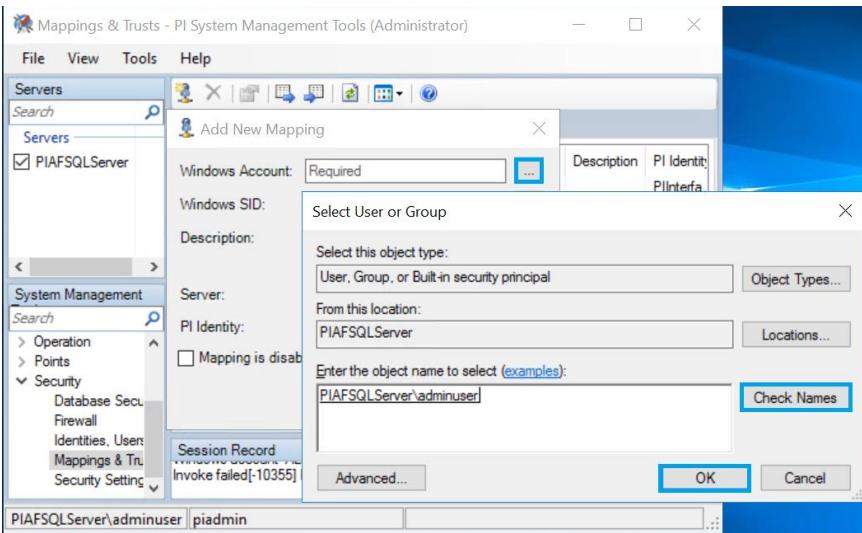
15. Browse the directory in **PI Identity** section, then select **PI groups** under the **Type** dropdown and Select **piadmins** to create PI Identity as **piadmins**.



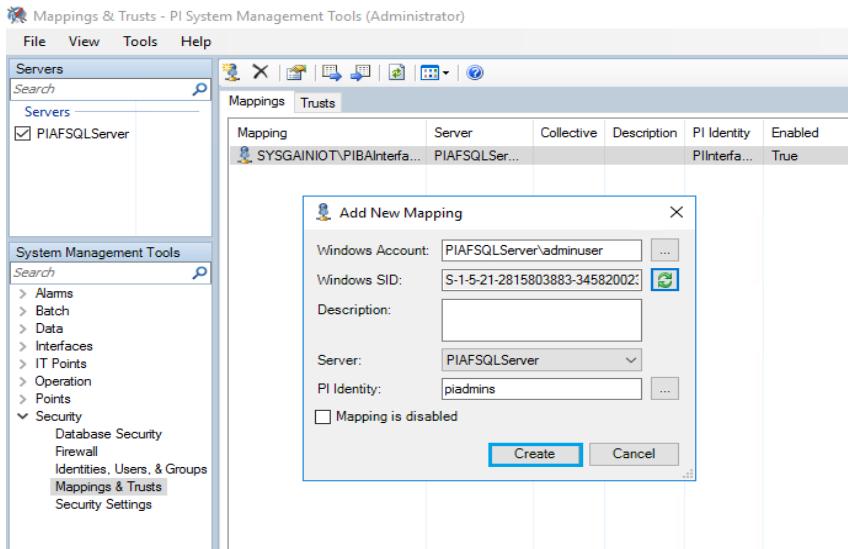
16. Click the dots next to **Windows Account**, then **Locations**, and select the **PIAFSQLServer**.  
Click on **OK**.



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

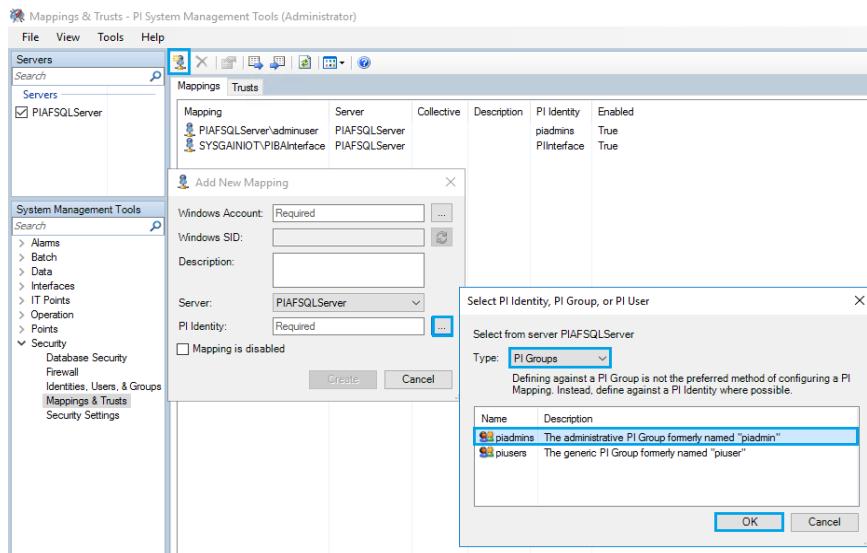


18. Click **Create**

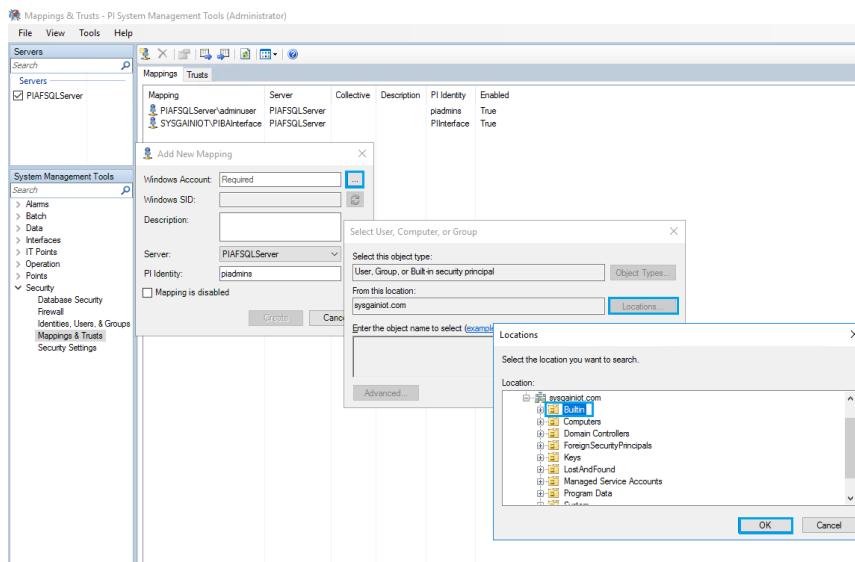


19. Create a new Mapping for **Administrator**.

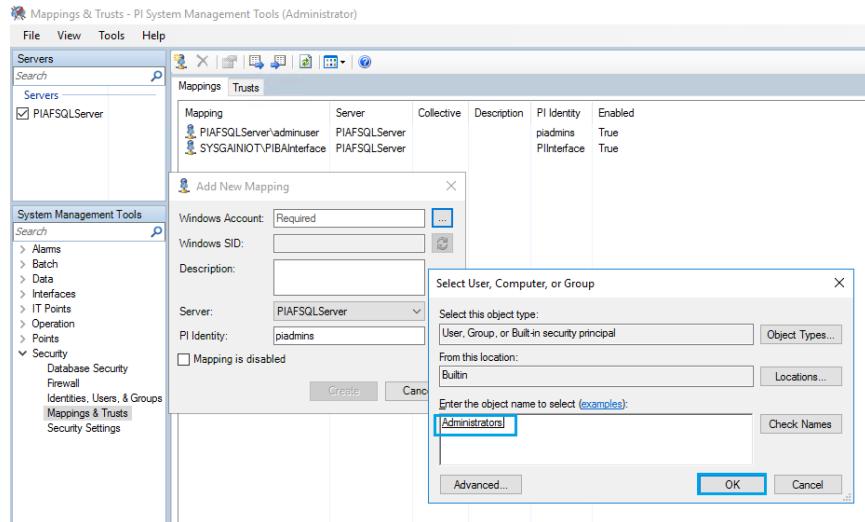
20. Near **PI Identity**, select **Type as PI Groups** > Select **piadmins** > Click on **OK**.



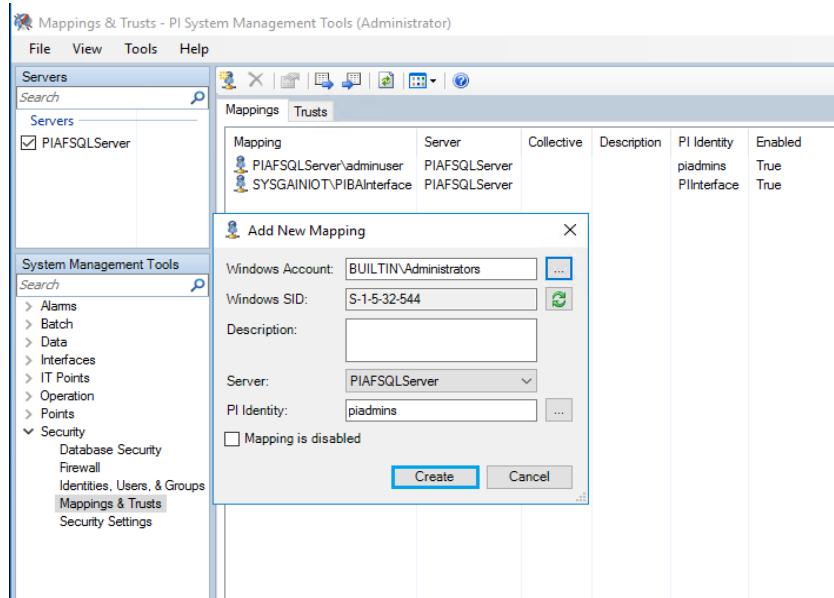
21. Click the Browse dots near **Windows Account** > Select **Locations** > click on **sysgaiiot.com**  
 > Select **Builtin** > Click **OK**.



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.

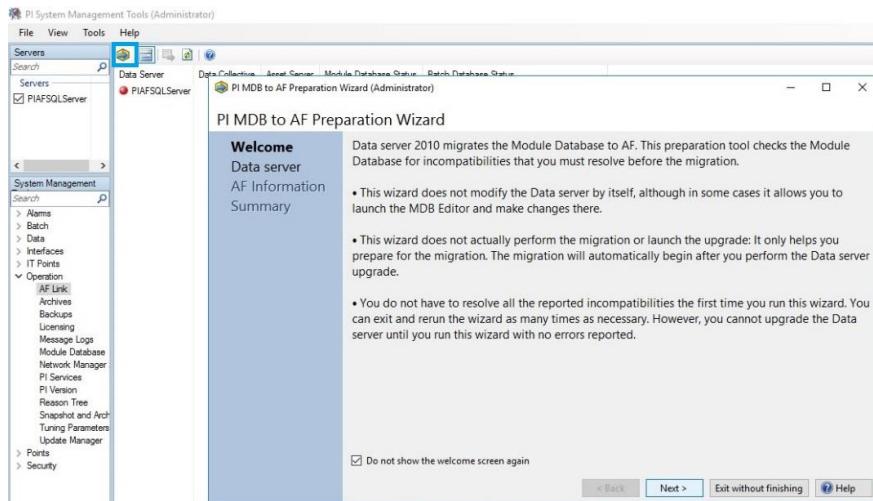
## 9.8. Prepare Data Server For Module Database(Mdb) To Asset Framework(AF)

Commented [UD43]: MDB – use full form for MDB and AF

Commented [KO44R43]: updated

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

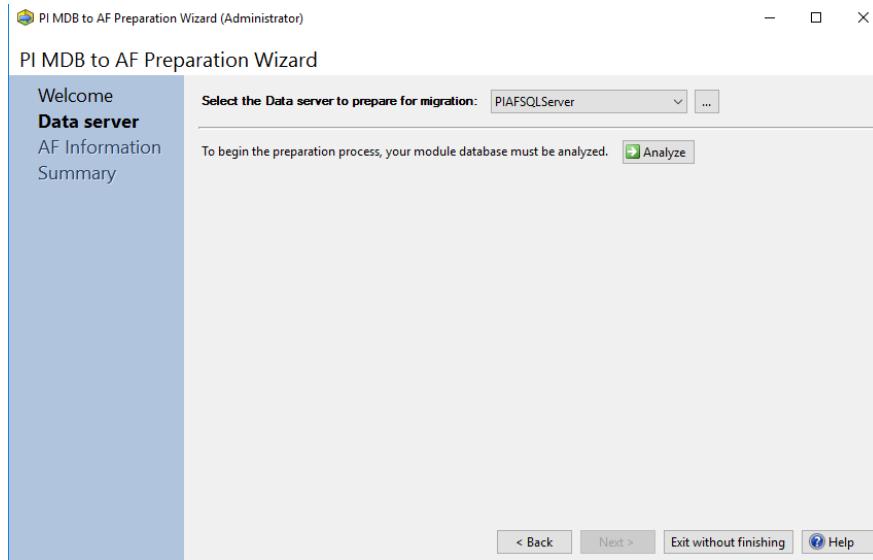
2. Click on **MDB to AF synchronization Wizard** (the symbol just below the **Help** tab). It will open the PI MDB to AF Preparation Wizard as shown below. Click on **Next**.

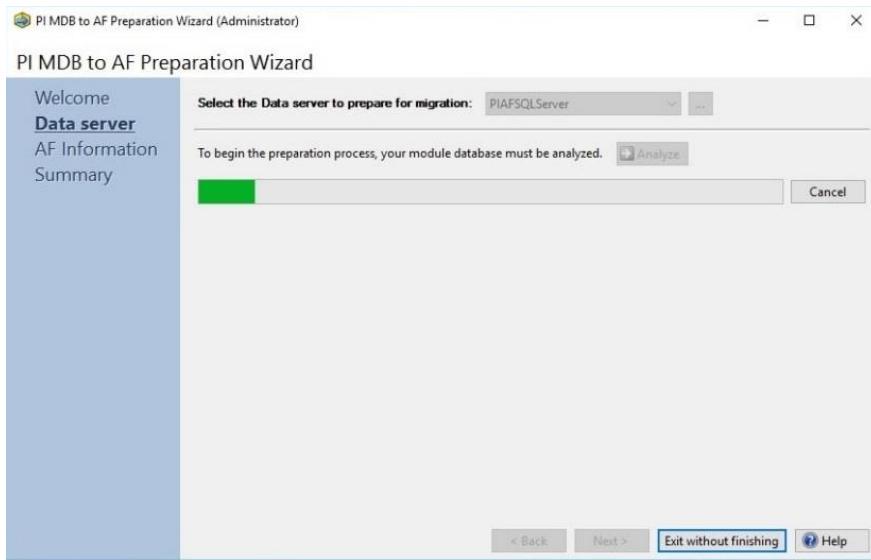


**Commented [UD45]:** Is the below image correct for this text??.... It seems like they don't match

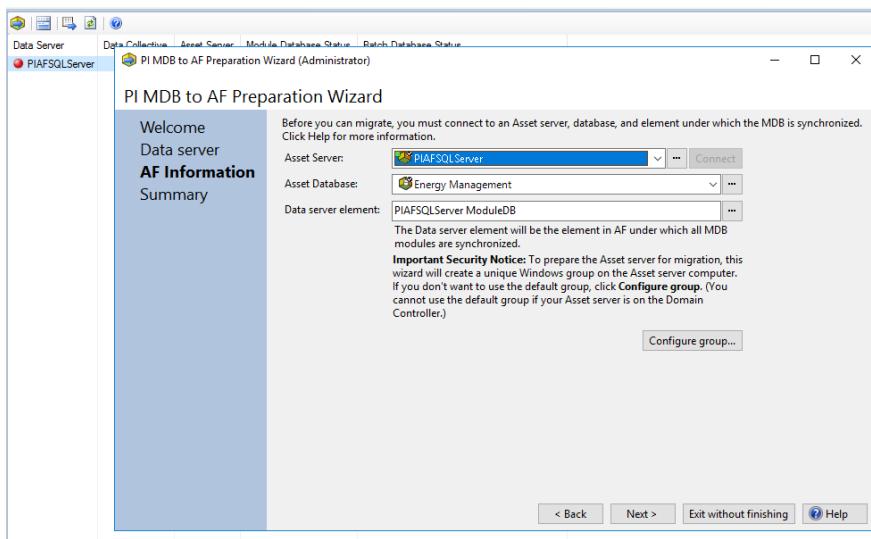
**Commented [KO46R45]:** This is correct image.i highlighted that symbol with blue.when we click on that it open that PI MDB to AF preparation wizard

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

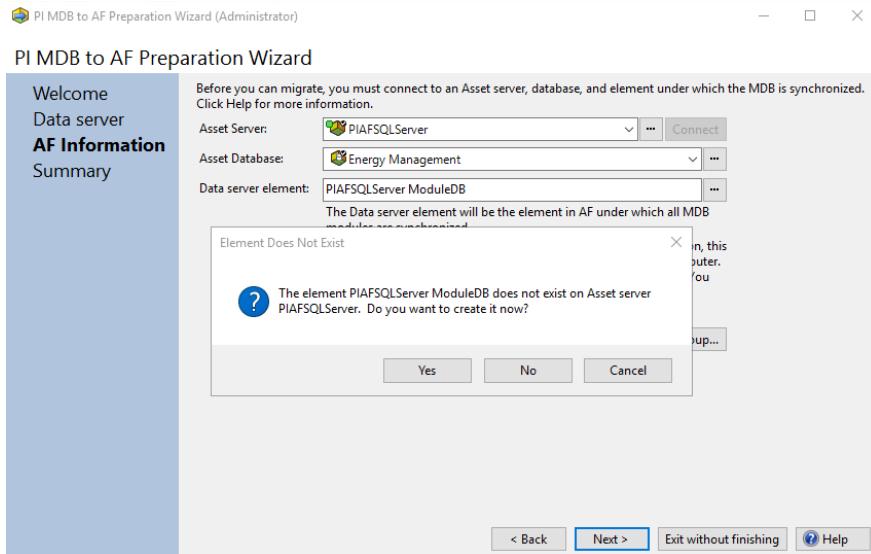




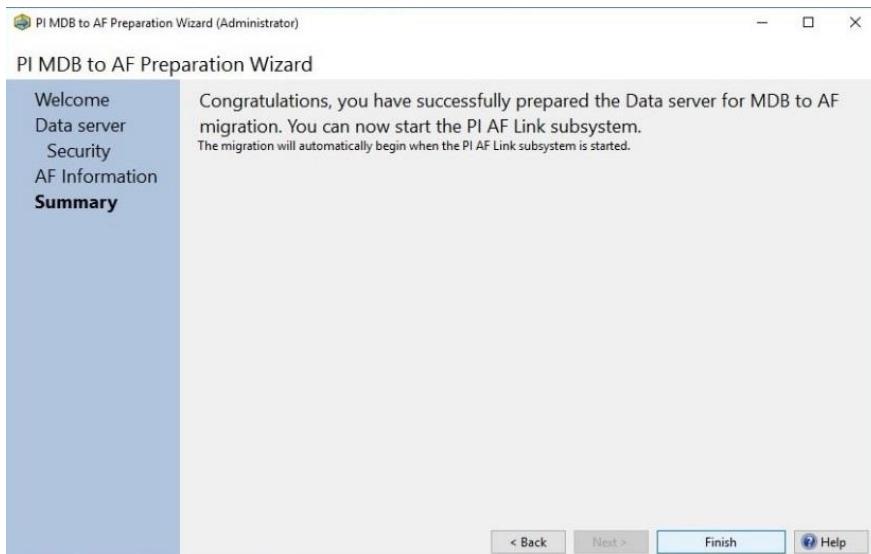
4. In AF Information, set the **Asset Server** as **PIAFSQLServer**, then click on **Connect**. Set **Asset Database** as **Energy Management**. Click on **Next**.

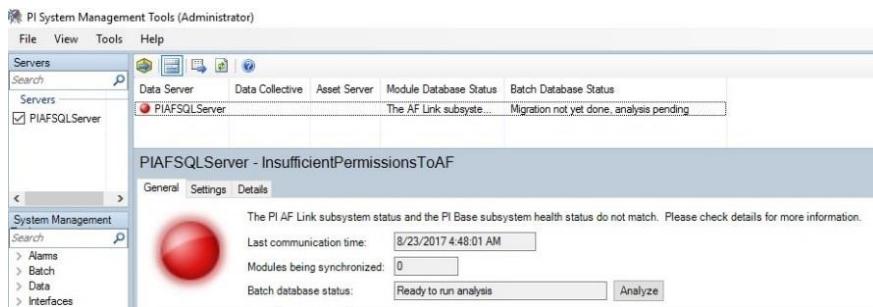


5. Click on **Yes** to create a PIAFSQLServer ModuleDB, then click on **Next**.

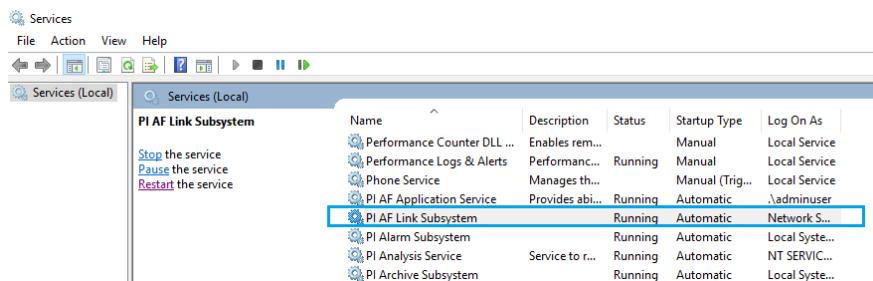


6. Click on **Finish**.

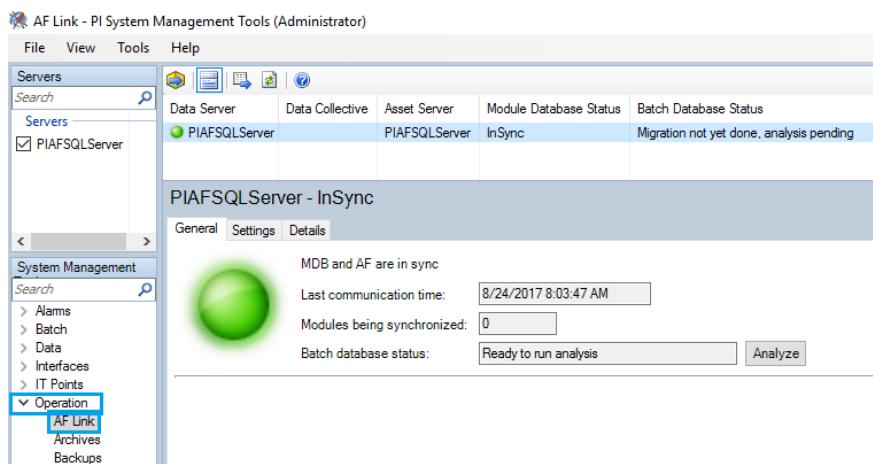




7. If you see the red circle on PIAFSQL Server, go to the **Services.msc** and restart the service **PI AF Link Subsystem**.

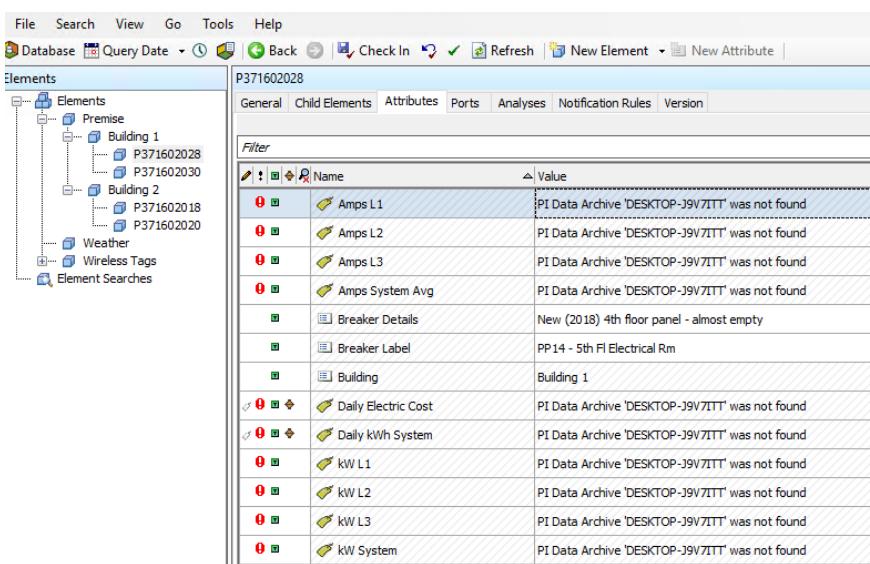


8. After restart, go to the **Operations** under system management and click on **AF Link**. You can see the PIAFSQL Server now has a green circle.



## 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.

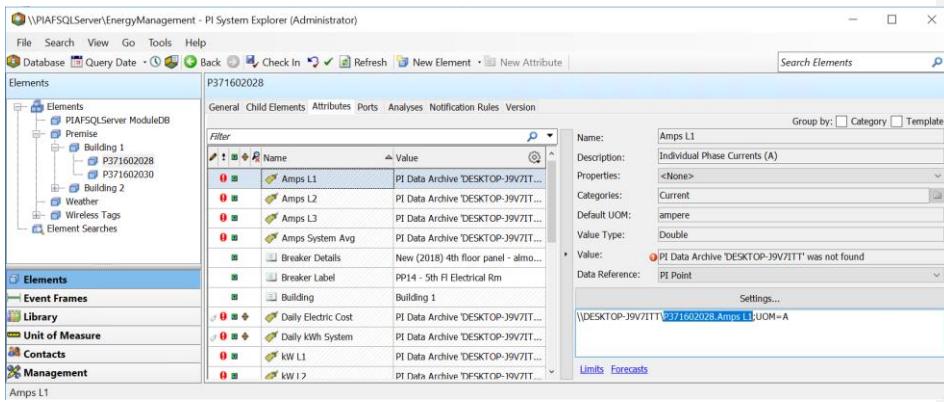


3. To update the attribute, click on a **Name**. Then, under Settings, copy the PI point as shown below.

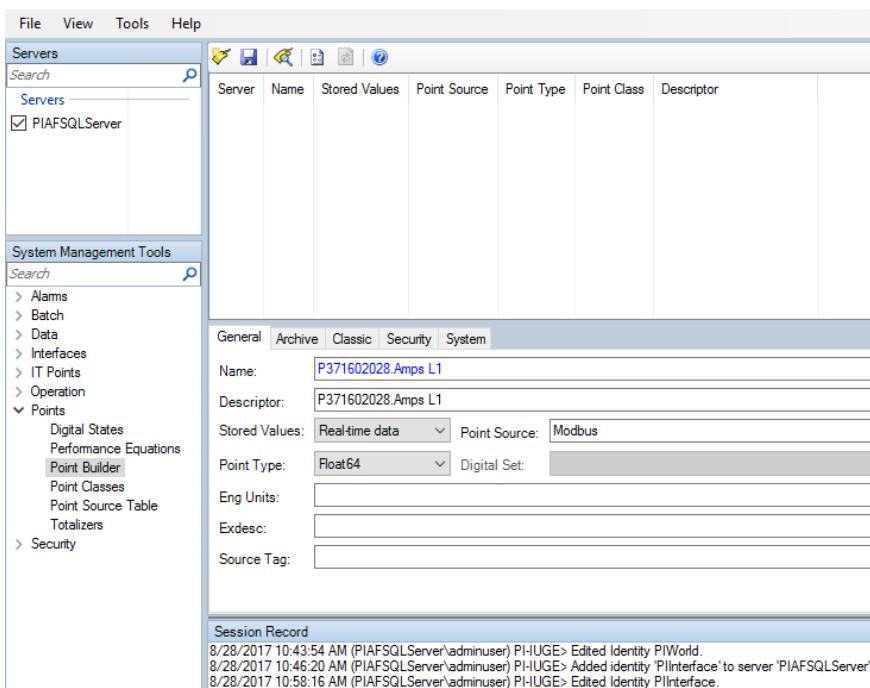
For example1, \\DESKTOP-J9V7ITT\P371602028.Amps L1;UOM=A  
the highlighted part (the text between "\\" and ";").

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**.

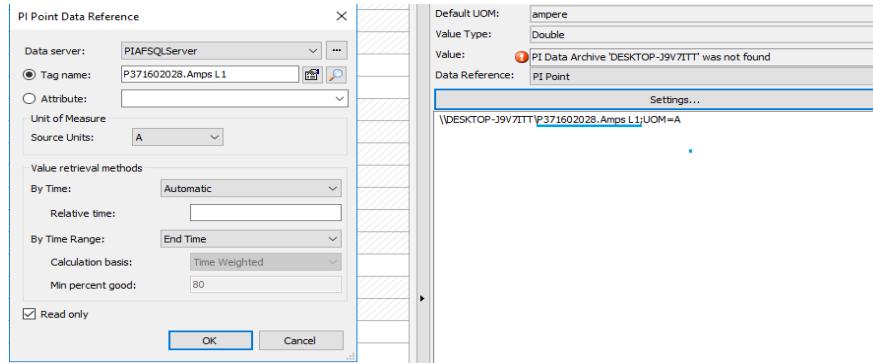


**Commented [UD47]:** Pls mention in which screen are you pasting and how would you go to that screen (if you are pasting it other than on Pi explorer)

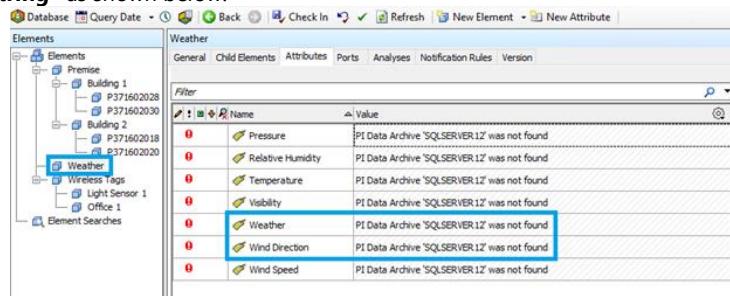
**Commented [KO48R47]:** Mentioned in point 4



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



Servers

Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor
PIAFSQLServer	P371602028 Amps L1	Real-time data	Modbus	Float64	classic	P371602028 Amps L1
PIAFSQLServer	P371602028 Amps L2	Real-time data	Modbus	Float64	classic	P371602028 Amps L2
PIAFSQLServer	P371602028 Amps L3	Real-time data	Modbus	Float64	classic	P371602028 Amps L3
PIAFSQLServer	P371602028 Amps System Avg	Real-time data	Modbus	Float64	classic	P371602028 Amps System Avg
PIAFSQLServer	P371602028 Daily Electric Cost 60e6094f-e554-5e0f-1742-54def61fbbe91	Real-time data	Modbus	Float64	classic	P371602028 Daily Electric Cost
PIAFSQLServer	P371602028 Daily kWh System 3b57c63ad3c7-9b43-1d9b-4d7994c899bc	Real-time data	Modbus	Float64	classic	P371602028 Daily kWh System
PIAFSQLServer	P371602028 Daily kW L1	Real-time data	Modbus	Float64	classic	P371602028 Daily kW L1
PIAFSQLServer	P371602028 Daily kW L2	Real-time data	Modbus	Float64	classic	P371602028 Daily kW L2
PIAFSQLServer	P371602028 Daily kW L3	Real-time data	Modbus	Float64	classic	P371602028 Daily kW L3
PIAFSQLServer	P371602028 kW System	Real-time data	Modbus	Float64	classic	P371602028 kW System
PIAFSQLServer	P371602028 Months Elapsed-Curr 10.120000_099E-17_0973k-44C04	Real-time data	Modbus	Float64	classic	P371602028 Months Elapsed-Curr

System Management Tools

- Alarms
- Batch
- Data
- Interfaces
- IT Points
- Operation
- Points
  - Digital States
  - Performance Equations
  - Point Builder**
  - Point Classes
  - Point Source Table
  - Totalizers
- Security

General Archive Classic Security System

Name: **NWS\_KFNL\_WindDirection**

Descriptor:

Stored Values: Real-time data Point Source: Modbus

Point Type: **String** Digital Set:

Eng Units:

Exdesc:

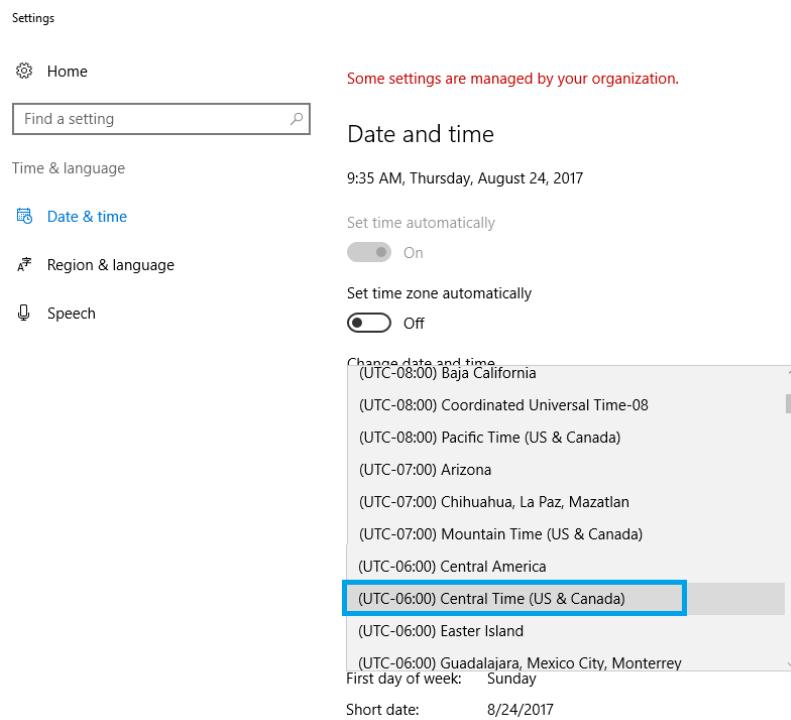
Source Tag:

Session Record

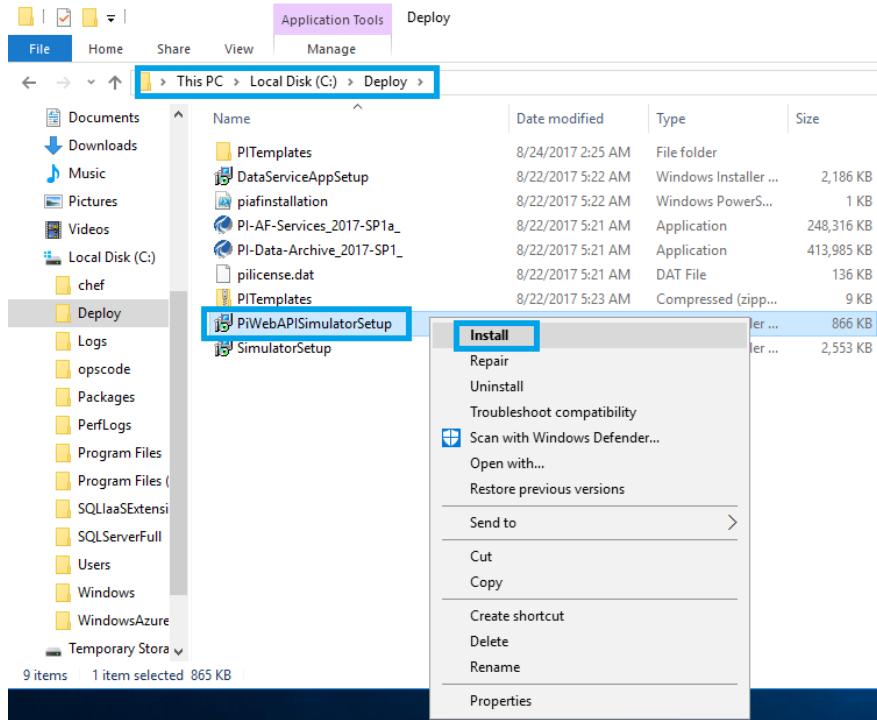
```
0/28/2017 12:32:04 PM (PIAFSQLServer\administrator) P1-PB: Successfully created point P37160202030 Volts L2 to Neutral on server PIAFSQLServer.
0/28/2017 12:32:19 PM (PIAFSQLServer\administrator) P1-PB: Successfully created point P37160202030 Volts L3 to Neutral on server PIAFSQLServer.
0/28/2017 12:34:22 PM (PIAFSQLServer\administrator) P1-PB: Successfully created point P37160202018 Amps L1 on server PIAFSQLServer.
0/28/2017 12:34:39 PM (PIAFSQLServer\administrator) P1-PB: Successfully created point P37160202018 Amps L2 on server PIAFSQLServer.
```

## 9.10. Install And Run The Piweb Simulator Setup

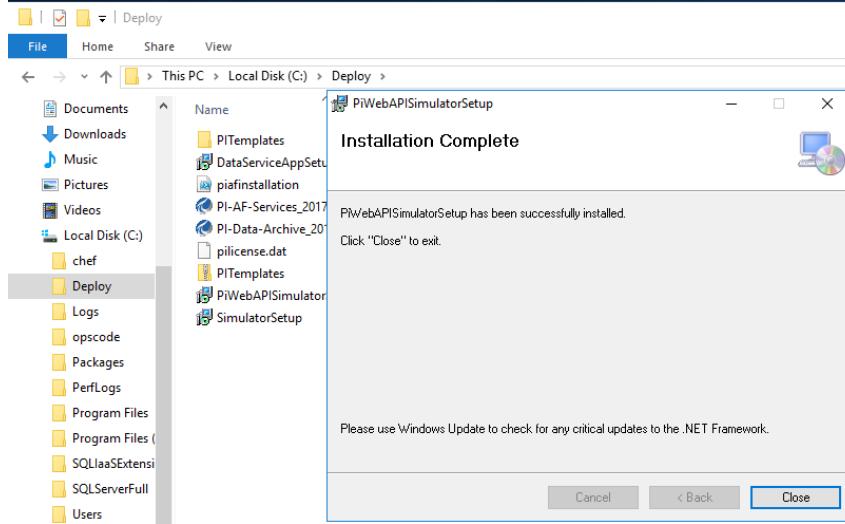
1. Change the time stamp to **(UTC-06:00) Central Time (US&Canada)**



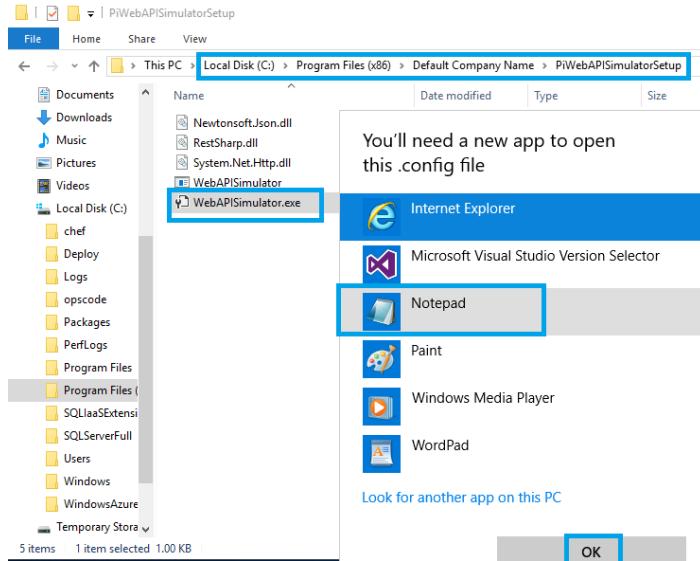
2. Navigate to the **Local Disk (C:) > Deploy > PIWebAPISimulatorSetup** and right-click to **Install**.



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\admininuser" />
<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**.

Commented [AS49]: Not to be hard coded

Commented [AS50]: From where do we get this value  
more info needed

Commented [KO51R50]: explained

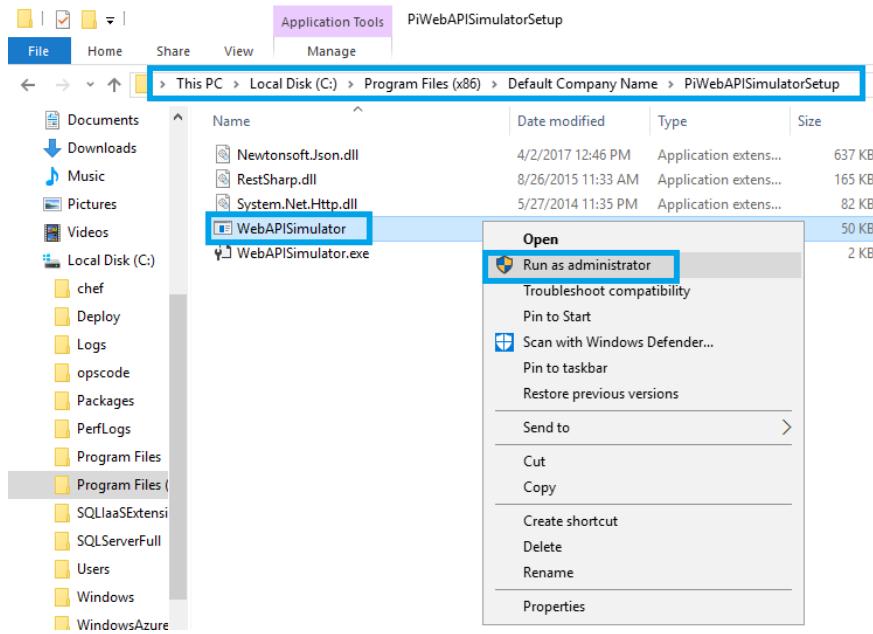
WebAPISimulator.exe - Notepad

```

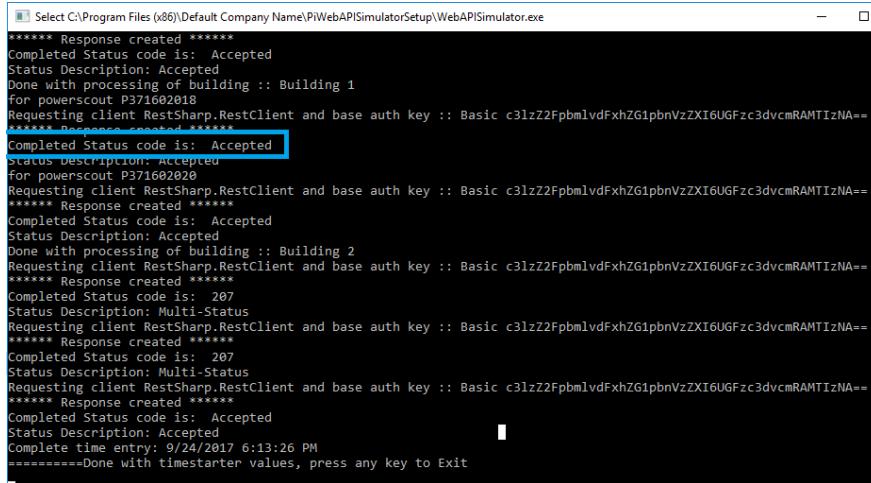
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
  </startup>
  <appSettings>
    <add key="UserName" value="sysgainiot\adminuser" />
    <add key="Password" value="Password@1234" />
    <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 c3lzZ2Fpbm1vdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
*****
Completed Status code is: Accepted
Status Description: Accepted
for powerscout P371602020
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2Fpbm1vdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
*****
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 c3lzZ2Fpbm1vdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
*****
Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2Fpbm1vdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
*****
Response created *****
Completed Status code is: 207
Status Description: Multi-Status
Requesting client RestSharp.RestClient and base auth key :: Basic c3lzZ2Fpbm1vdFjhZG1pbnVzZXi6UGFzc3dvcnRAMTizNA==
*****
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

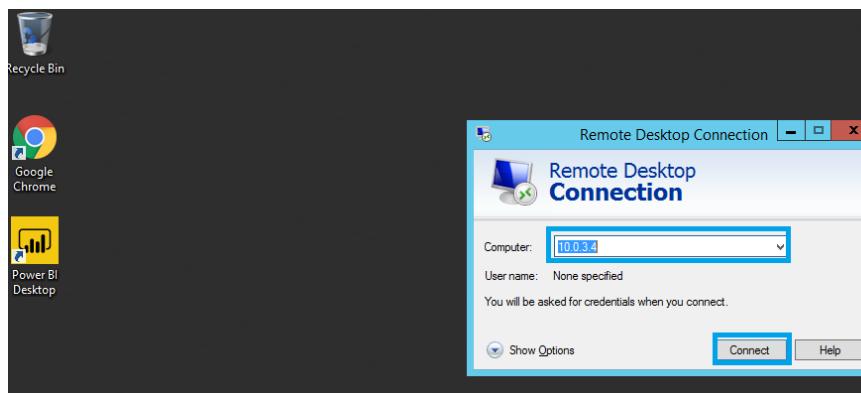
```

{
  "Links": {},
  "Items": [
    {
      "WebId": "DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90",
      "Id": "deela2d2-ac-4945-52e1-4a1e9ba3ddc",
      "Name": "Configuration",
      "Description": "Provides access for configuration data.",
      "Path": "\\\PIAFSQLServer\configuration",
      "ExtendedProperties": {},
      "Links": {},
      "Self": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90",
      "Elements": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/el",
      "ElementTemplate": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/elt",
      "EventFrames": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/e",
      "AssetServer": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetserver/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90",
      "AttributeCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/act",
      "AttributedCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/act",
      "TableCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/t",
      "AnalyticalCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/a",
      "Tables": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/tabc",
      "EnumerationSets": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/enum",
      "Tables": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/tabc",
      "Security": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/sec",
      "SecurityEntries": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gLabh3qyeRIMcC4Ucem6qdjgUE1BR1NRTFNFU12FU1xDT05GSDvU7kFUSU90/sec"
    },
    {
      "WebId": "W0074e00818000d8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU",
      "Id": "15327246-d4f2-44ab-96ab-f4f4b0be250e",
      "Name": "EnergyManagement",
      "Description": "",
      "Path": "\\\PIAFSQLServer\EnergyManagement",
      "ExtendedProperties": {},
      "Links": {},
      "Self": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU",
      "Elements": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/elt",
      "ElementTemplate": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/elt",
      "EventFrames": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/e",
      "AssetServer": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetserver/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU",
      "AttributeCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/act",
      "AttributedCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/act",
      "TableCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/t",
      "AnalyticalCategories": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/a",
      "Tables": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/tabc",
      "EnumerationSets": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/enum",
      "Tables": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/tabc",
      "Security": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/sec",
      "SecurityEntries": "https://plafsqlserver.sysgauntlet.com/piwebapi/assetdatabases/DO1exX0kjSWWUk8kLewWh7I7gKXXSGFP0Ug0a2q49EvL41DgUE1BR1NRTFNFU12FU1xFTkVSR11NQ5BBDvVNRSU/sec"
  ]
}

```

## 10. Installation of PI BA Integrator

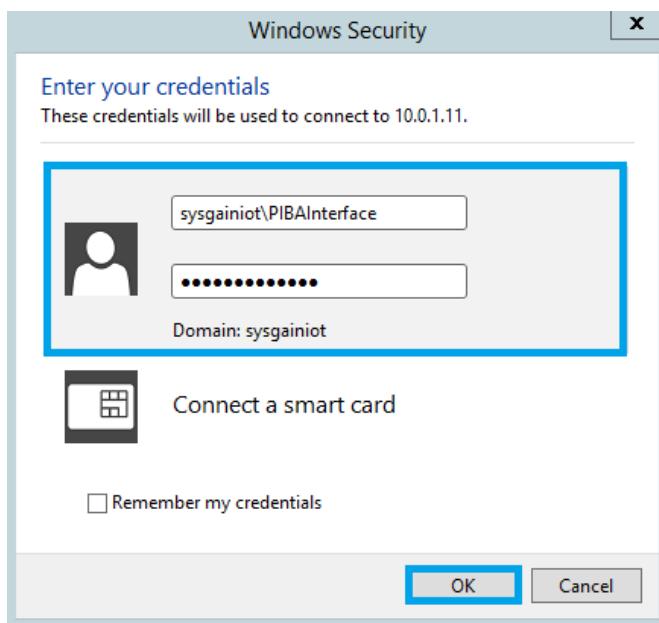
1. From Bastion server, connect to the Remote server PIBA VMserver with details provided in output section.



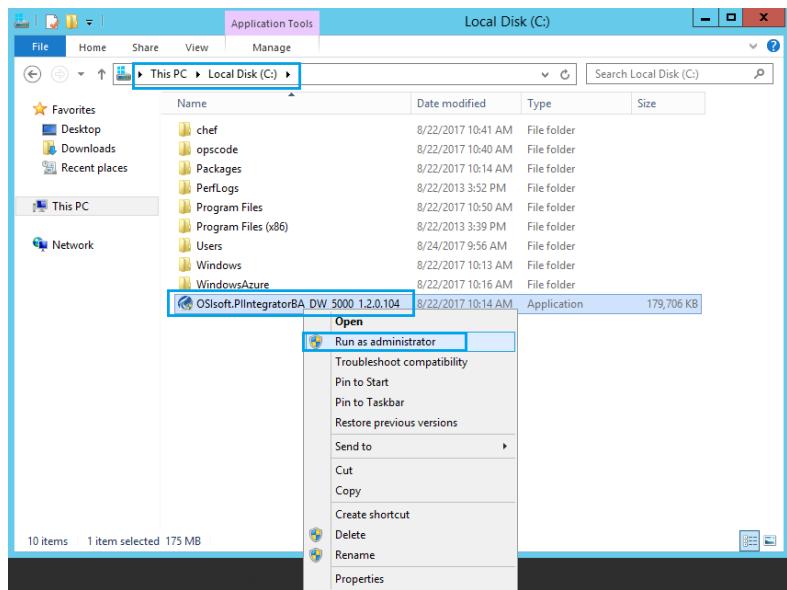
Commented [AS52]: Update with which credentials to login to PIBA server.

Commented [SN53R52]: updated

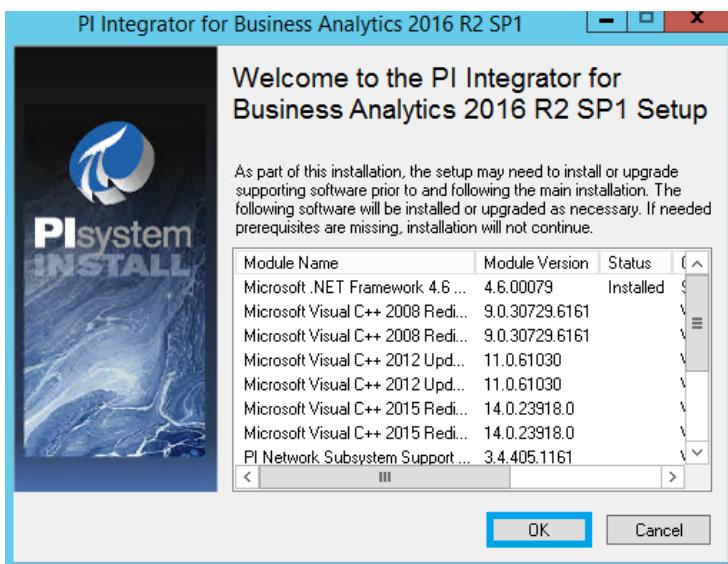
2. Login with credentials "<domainname>\PIBAInterface"( user you created in AD server) and **password**.



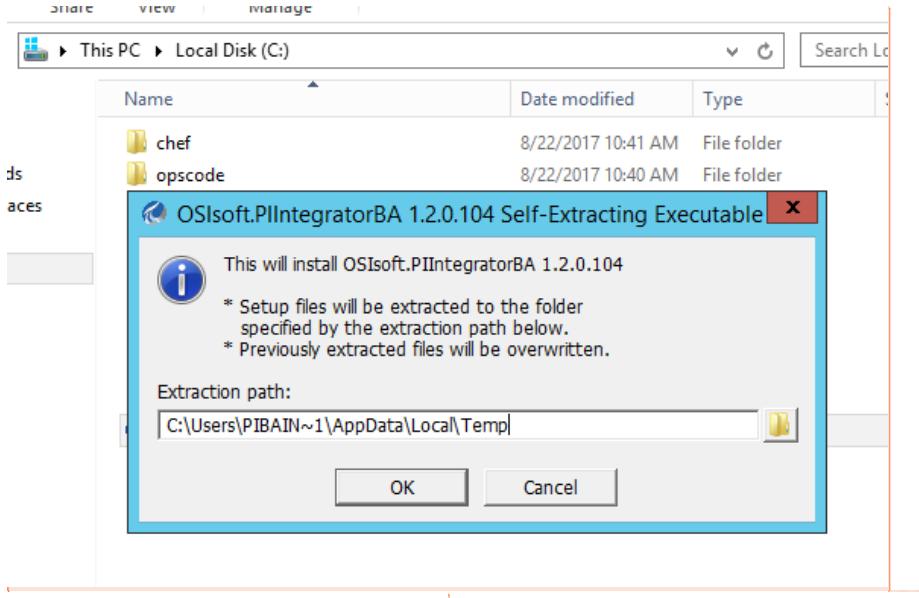
3. After connecting to the PIBA VMServer, navigate to the LocalDisk (C:) and select **OSISoft.PIIntegratorBA**, then right-click on and **Run as administrator**.



4. Click on **Ok**.



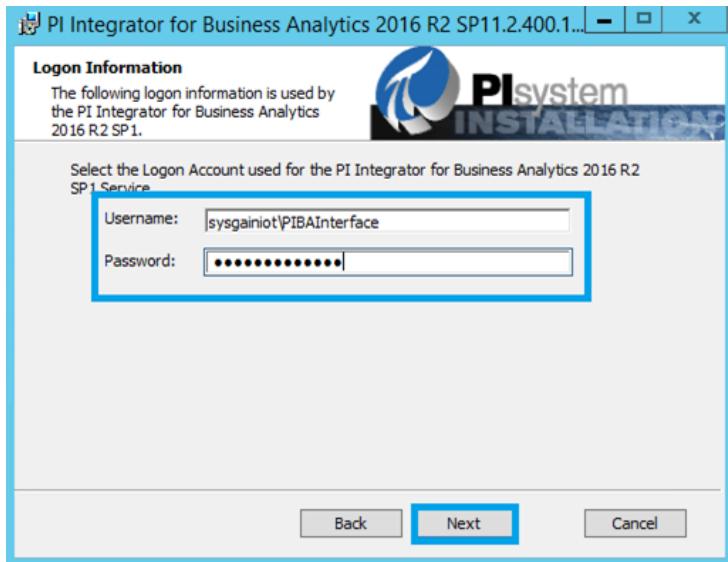
5. Click on **OK**



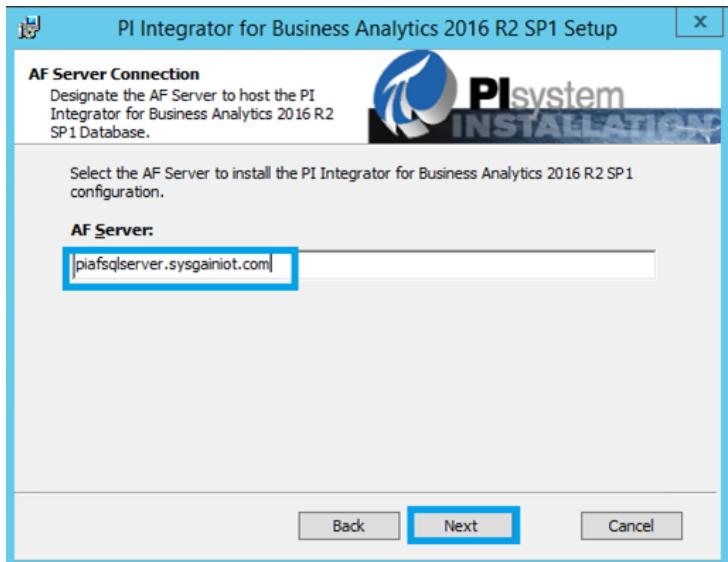
Commented [AS54]:

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

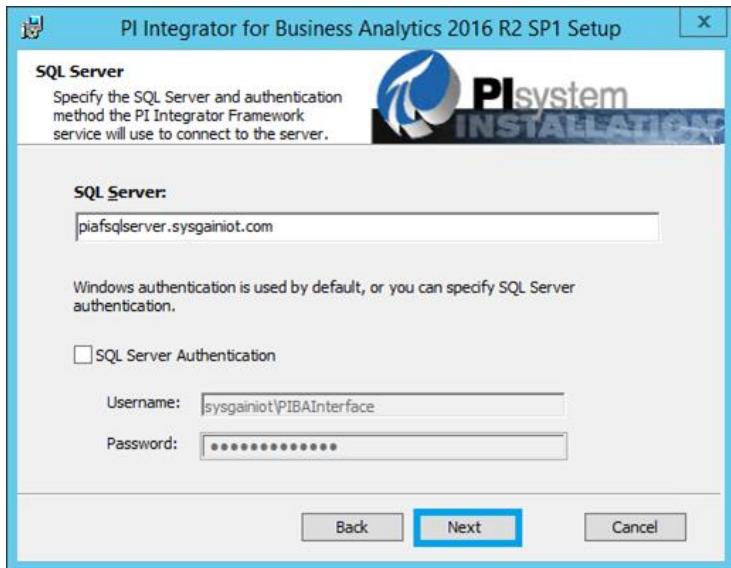
Commented [AS55R54]: Logon Information screenshot and details to it



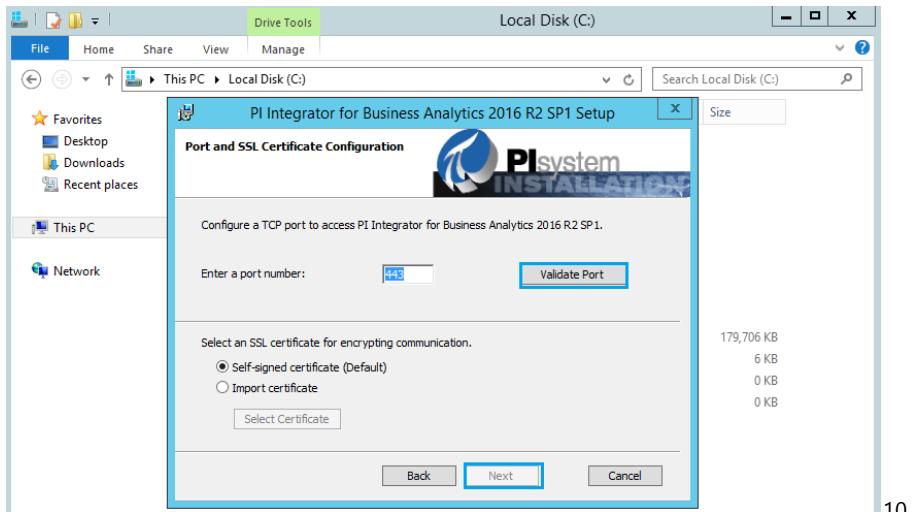
7. Give the Af sever link as piafsqlserver.<domainname> to host PIBA database and click on **Next**



Click on **Next**

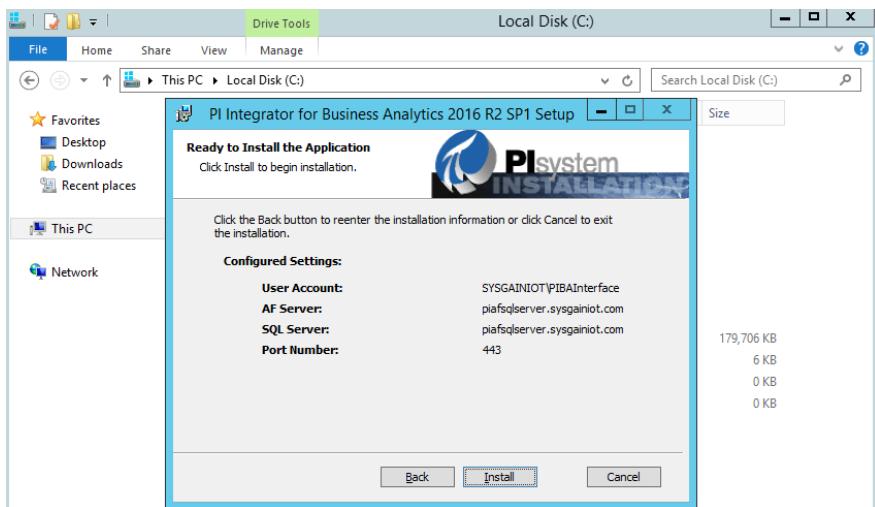


8. Click on **Validate port**, then **Next**.



Click on **Install**.

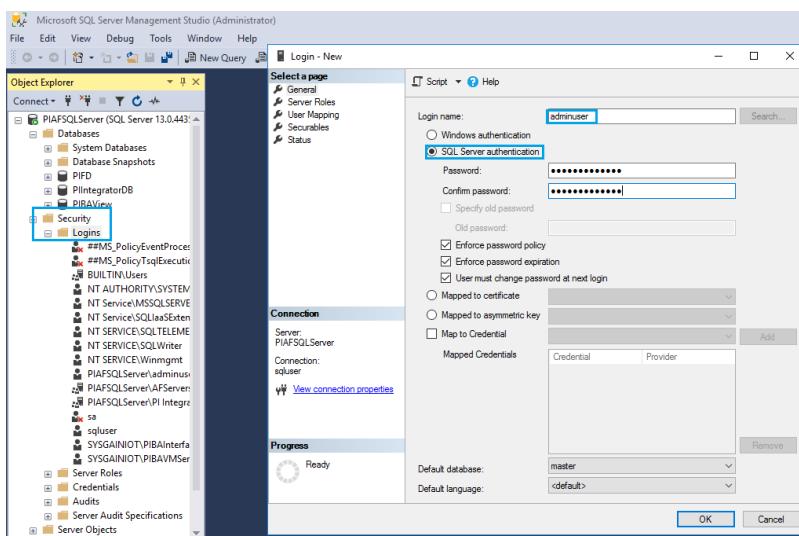
10.



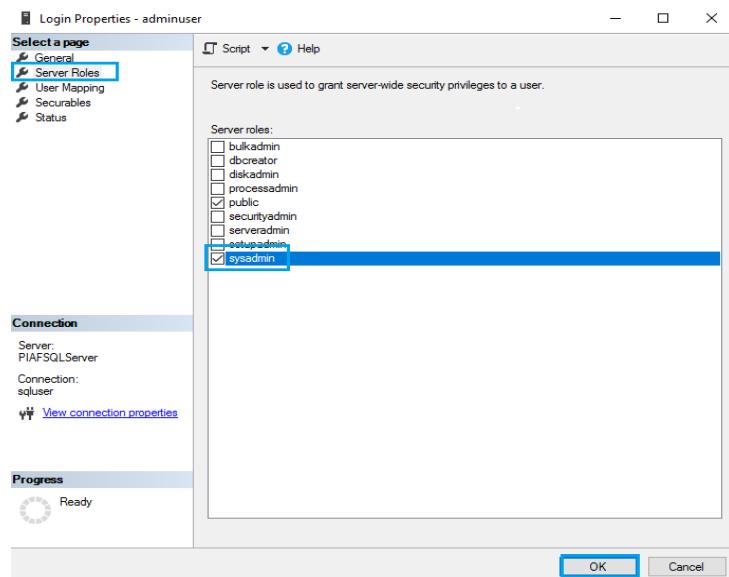
## 10.1. Configuring PI Business Analytics

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

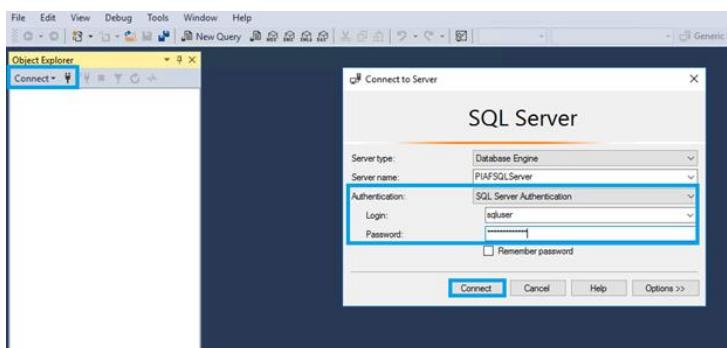
2. Go to the **Security** section, then right-click on **Login** and select **New Login**. Set the login name as **adminuser** and select **SQL Server Authentication**. Set a password, then click on **Ok**.



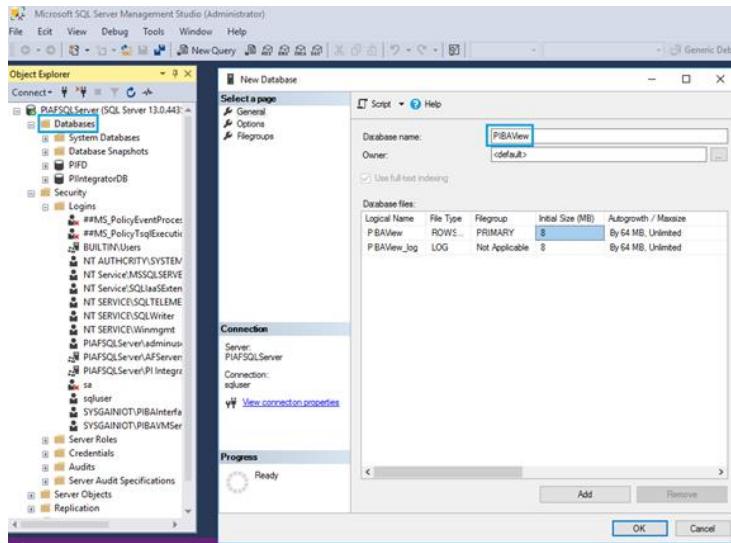
3. Right-click on the admin user under **Login** and select **Properties**. On the Properties screen, select **Server Roles**, then check **sysadmin** and click **Ok**.



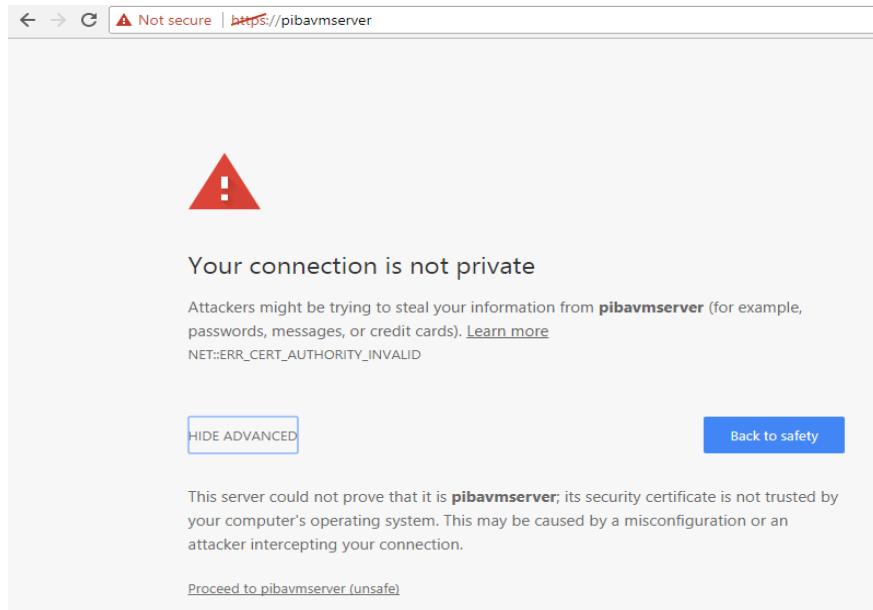
4. Disconnect and Click on connect in **ssms** to login with SQL Servr authentication to create database with following SQL credentials



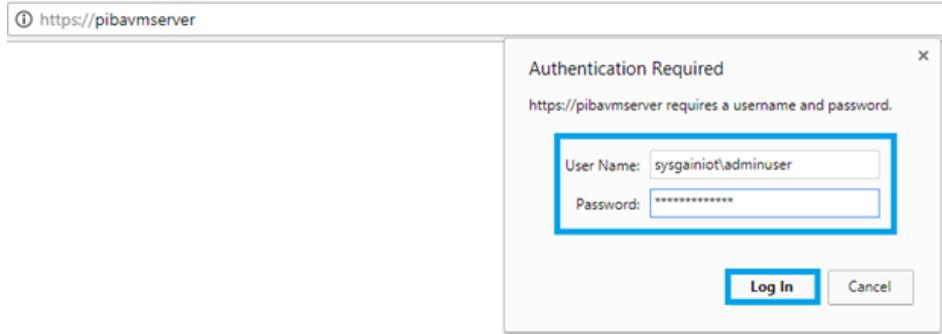
5. Go to the **SQLServer Management Studio**, right-click on **Database**, select **New Database**, and give the Database name as **PIBAView**. Click on **Ok**.



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



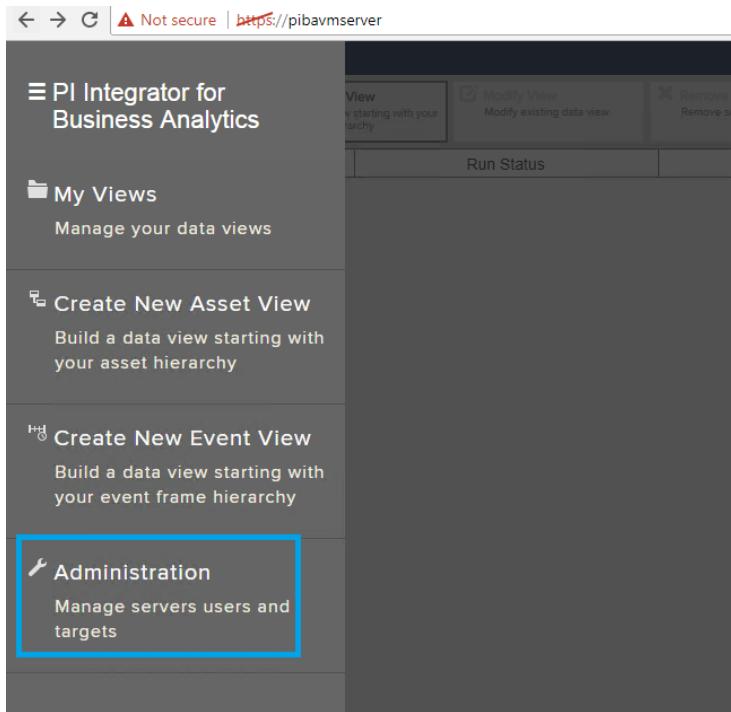
8. Click on **PI Integrator for Business Analytics** as shown below.

The screenshot shows a browser window with the URL <https://pibavmserver>. The page title is "PI Integrator for Business Analytics". It features a navigation bar with a menu icon and several buttons: "+ Create Asset View" (Build a data view starting with your asset hierarchy), "+ Create Event View" (Build a data view starting with your event frame hierarchy), "Modify View" (Modify existing data view), and "Remove View" (Remove selected view). Below these buttons is a table with columns: Lock, Name, Run Status, and Type. The table currently has one row with a lock icon and a blank name field.

Commented [AS56]: Add authentication required screenshot. I sent you in slack. And what creds to pass.

Commented [SN57R56]: updated

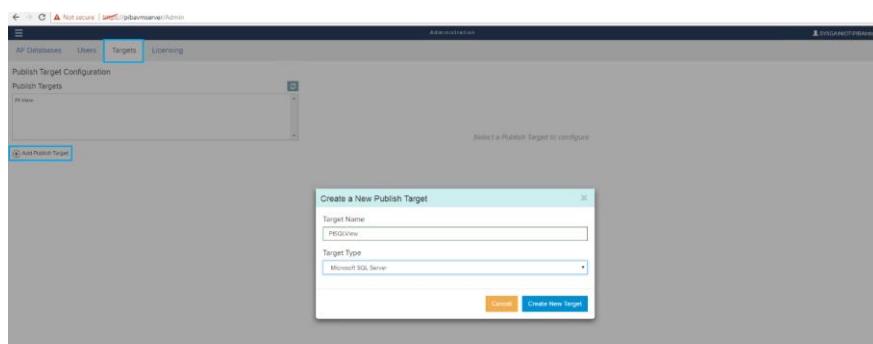
3. Click on **Administration**.



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

Enter Target Name as **PISQLView**.

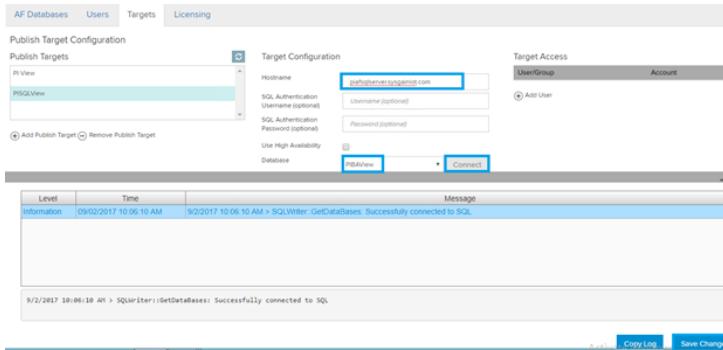
Select Target type as **Microsoft SQL Server** from drop down. After that click on create new target .



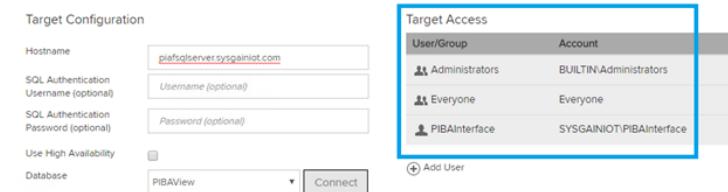
Commented [AS58]: Add a point for clicking create new target.

Commented [KO59R58]: updated

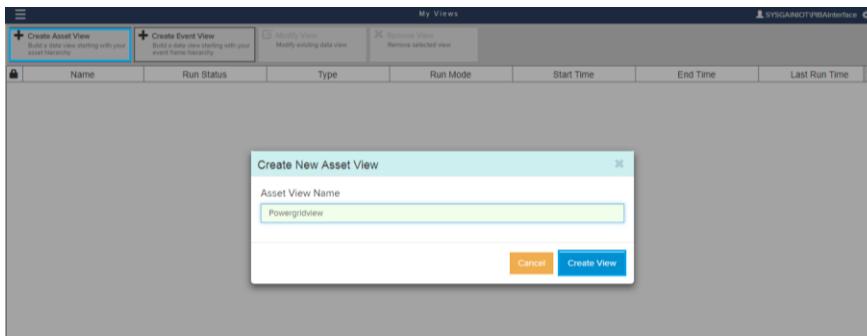
5. Enter the Hostname as **piafsqlserver.<domainname>** and click on connect and then select database you created in piaf ssms, select Database as **PIBAView** and **click on save changes**



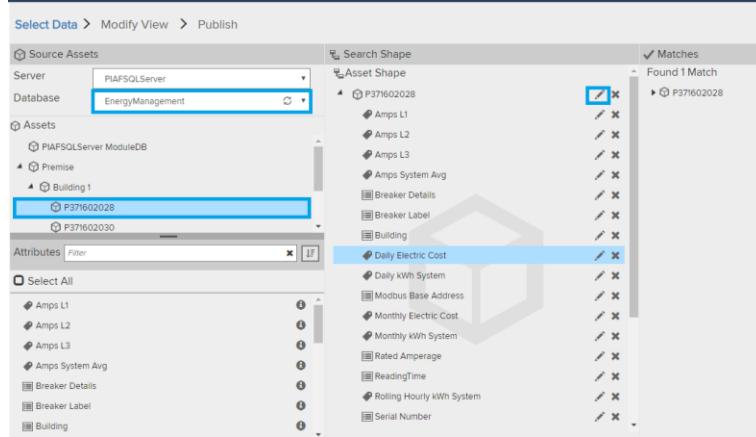
6. You can view the created **target access**



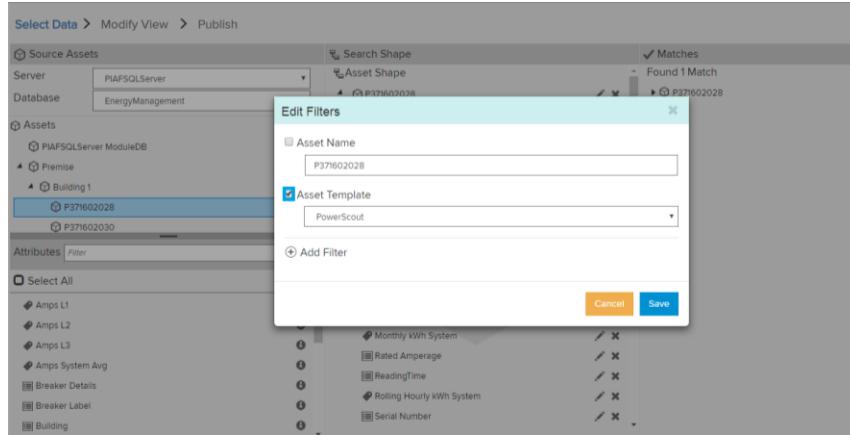
7. Click on **Create Asset view**. Set the Asset View Name as **PowergridView** and click on **Create View**.



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



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



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

Select Data > Modify View > Publish

Source Assets

Server: PIAFSQLServer  
Database: EnergyManagement

Assets

- PIAFSQLServer ModuleDB
- Premise
- Building 1
  - P371602028**
  - P371602030

Attributes: Filter

Select All

- Amps L1
- Amps L2
- Amps L3
- Amps System Avg
- Breaker Details
- Breaker Label
- Building
- Daily Electric Cost
- Daily kWh System
- Modbus Base Address
- Monthly Electric Cost
- Monthly kWh System
- Rated Amperage
- ReadingTime
- Rolling Hourly kWh System
- Serial Number
- Building

Search Shape

Asset Shape

Found 4 Matches

- PowerScout
  - Amps L1
  - Amps L2
  - Amps L3
  - Amps System Avg
- Breaker Details
- Breaker Label
- Building
- Daily Electric Cost
- Daily kWh System
- Modbus Base Address
- Monthly Electric Cost
- Monthly kWh System
- Rated Amperage
- ReadingTime
- Rolling Hourly kWh System
- Serial Number
- Building

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

Select Data > Modify View > Publish

Add Column 26 columns

Edit Row Filters 0 Row Filters

Edit Value Mode Interpolated Values Every 1 Minutes

Start Time: 8/24/2017 3:31:27 AM End Time: 8/24/2017 3:48:27 AM Apply

PowerScout	TimeStamp	Amps L1	Amps L2	Amps L3	Amps System Avg	Breaker Data
P371602028	8/24/2017 3:31:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:32:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:33:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:34:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:35:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:36:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:37:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:38:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:39:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:40:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:41:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:42:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:43:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:44:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:45:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:46:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:47:27 AM					New (2018) 4th floor pi
P371602028	8/24/2017 3:48:27 AM					New (2018) 4th floor pi

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

Select Data > Modify View > Publish

**Edit Value Mode**

Sampled Values

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

**Save Changes**

Powerscout	Timestamp	Amps L1	Amps L2	Amps L3	Amps System Avg	Breaker Data
P371602018	8/24/2017 4:44:07.916 AM	100.374	100.545	100.243	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:45:07.804 AM	60.528	60.528	60.528	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:46:07.679 AM	20.813	20.813	20.813	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:47:07.546 AM	112.100	112.100	112.100	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:48:07.413 AM	93.819	93.819	93.819	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:49:07.263 AM	91.097	91.097	91.097	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:49:42.153 AM	30.298	30.298	30.298	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:50:07.088 AM	109.811	109.811	109.811	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:50:42.042 AM	37.587	37.587	37.587	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:51:06.902 AM	16.956	16.956	16.956	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:51:41.923 AM	128.875	128.875	128.875	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:52:06.769 AM	110.243	110.243	110.243	New (2013) 3rd floor pi	
P371602018	8/24/2017 4:52:41.806 AM	67.251	68.049	67.725	67.725	New (2013) 3rd floor pi
P371602018	8/24/2017 4:53:06.645 AM	70.054	70.866	70.528	70.528	New (2013) 3rd floor pi
P371602018	8/24/2017 4:53:41.689 AM	27.813	28.144	28.009	28.009	New (2013) 3rd floor pi
P371602018	8/24/2017 4:54:06.530 AM	77.272	78.190	77.817	77.817	New (2013) 3rd floor pi
P371602018	8/24/2017 4:54:41.571 AM	35.051	35.468	35.298	35.298	New (2013) 3rd floor pi
P371602018	8/24/2017 4:55:06.414 AM	37.835	38.284	38.102	38.102	New (2013) 3rd floor pi

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

Select Data > Modify View > Publish

**Target Configuration**

PISQLView

Run Once

Run on a Schedule

First Run

\*

Recur every  minutes

**Summary**

Shape and Matches

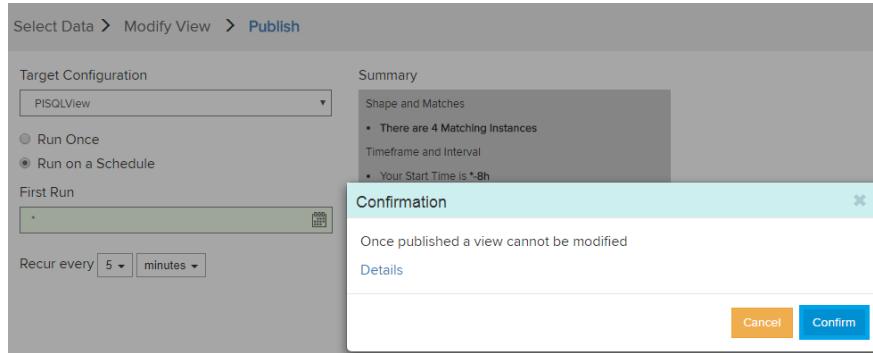
- There are 4 Matching Instances

Timeframe and Interval

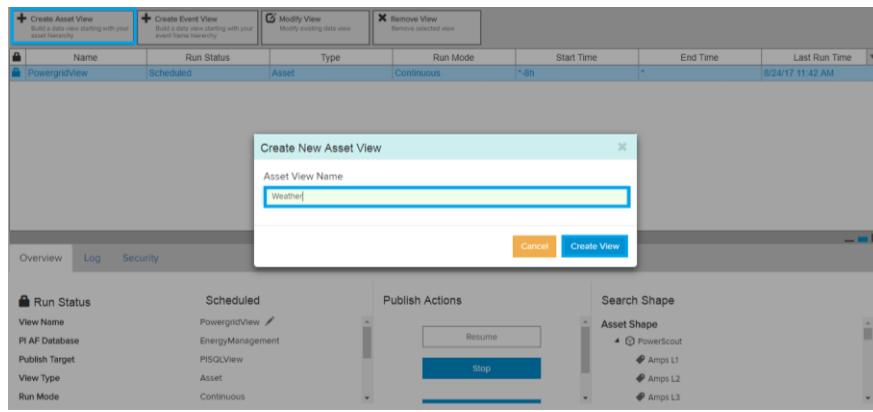
- Your Start Time is \*-8h
- Your End Time is \*
- Your Time Interval gets an interpolated measurement based on column Amps L1

**Publish**

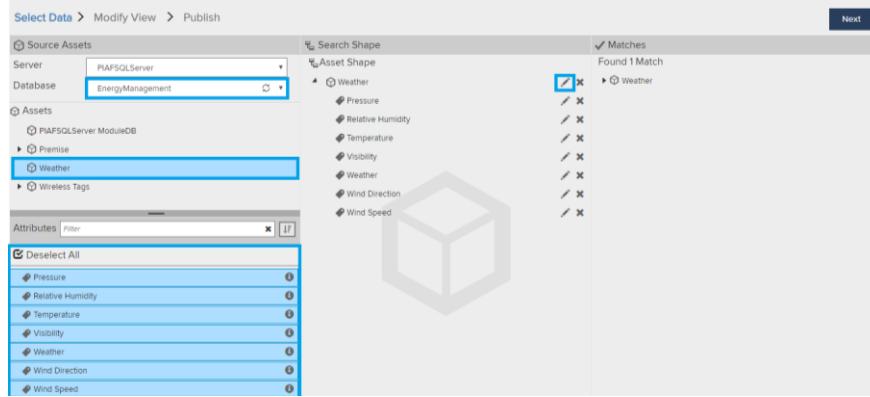
14. Click on **Confirm**.



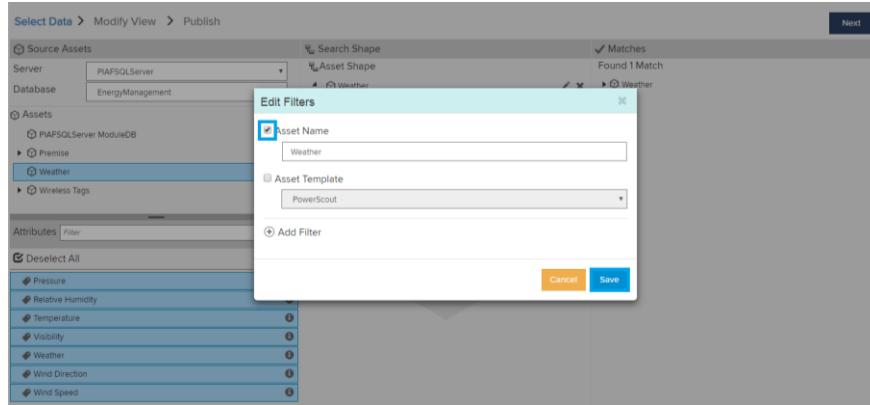
15. Create another Asset view by clicking on **Create asset view**, name it **Weather**, then click on **Create view**.



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



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



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

Select Data > Modify View > Publish

Source Assets

Server: PIAFSQLServer  
Database: EnergyManagement

Assets

- Premise
- Weather**
- Wireless Tags

Attributes

Deselect All

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

Search Shape

Asset Shape

Weather

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

Matches

Found 1 Match

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

Next

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

Select Data > Modify View > Publish

Add Column  
8 columns

Edit Row Filters  
0 Row Filters

Edit Value Mode  
Interpolated Values  
Raw and Precise

Start Time: End Time: Apply

Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather	Wind Direction	Wind Speed
Weather	8/2/2017 4:48:07.4...	29.207				Overcast	North	7.241	
Weather	8/2/2017 4:49:07.3...	31.213				Variable	Variable	19.281	
Weather	8/2/2017 4:49:22.2...	31.922				Light	Northwest	23.531	
Weather	8/2/2017 4:50:07.1...	29.220				North	North	7.320	
Weather	8/2/2017 4:50:42.1...	30.709				Mist	Southeast	15.235	
Weather	8/2/2017 4:51:05.9...	29.011				North	North	6.064	
Weather	8/2/2017 4:51:41.9...	30.932				Southeast	Southeast	17.590	
Weather	8/2/2017 4:52:05.8...	28.928				West	West	5.566	
Weather	8/2/2017 4:52:41.8...	29.719				Breezy	South	10.314	
Weather	8/2/2017 4:53:06.7...	31.715				in Vici	Northwest	22.290	
Weather	8/2/2017 4:53:41.7...	28.506				West	West	3.038	
Weather	8/2/2017 4:54:06.5...	31.938				Light	Northwest	23.625	
Weather	8/2/2017 4:54:41.6...	30.639				Light Rain	Southeast	15.835	
Weather	8/2/2017 4:55:09.4...	28.160	65.982	72.929	6.598	Fog/Mist	East	0.960	
Weather	8/2/2017 4:55:41.5...	30.862	4.002	36.361	0.400	Light Rain	Southeast	17.171	
Weather	8/2/2017 4:56:05.3...	30.947	71.546	76.212	7.155	A Few Clouds	Southeast	17.685	
Weather	8/2/2017 4:56:41.3...	28.214	73.686	77.474	7.369	A Few Clouds	South	1.284	
Weather	8/2/2017 4:57:05.2...	29.735	0.349	37.156	0.535	unknown Precip	South	10.409	
Weather	8/2/2017 4:57:41.2...	28.437	43.369	59.588	4.337	Fair and Breezy	East	2.619	
Weather		10.913	40.439	1.091		A Few Clouds			

Edit Value Mode

Sampled Values

Use Key Column Pressure

Interpolate

Exact

Cancel Save Changes

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

Select Data > Modify View > Publish								
Add Column 9 columns		Edit Row Filters		Edit Value Mode Interpolated Value Edit Value				
				Start Time	End Time			
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 4:52:05.8...	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	4.296	Fair and Breezy	South	10.314
Weather	8/24/2017 4:53:06.7...	31.715	92.874	68.796	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 4:54:05.5...	31.938	98.438	92.078	9.844	Thunderstorm Light	Northwest	23.625
Weather	8/24/2017 4:54:41.6...	30.639	65.962	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  minutes

Summary

Shape and Matches

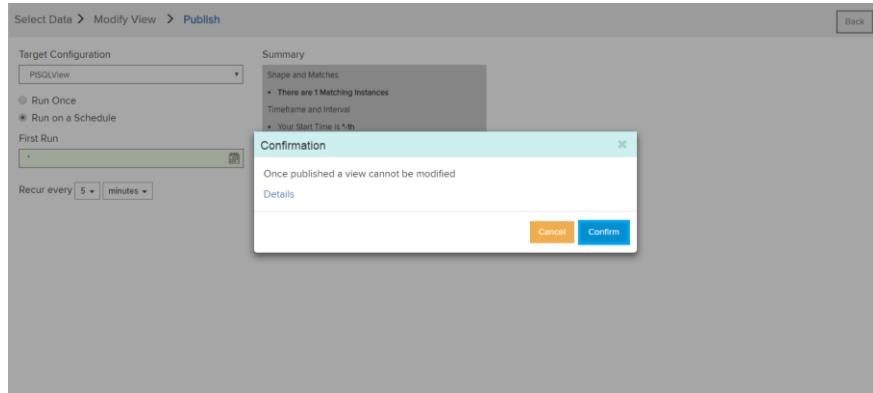
- There are 1 Matching Instances

Timeframe and Interval

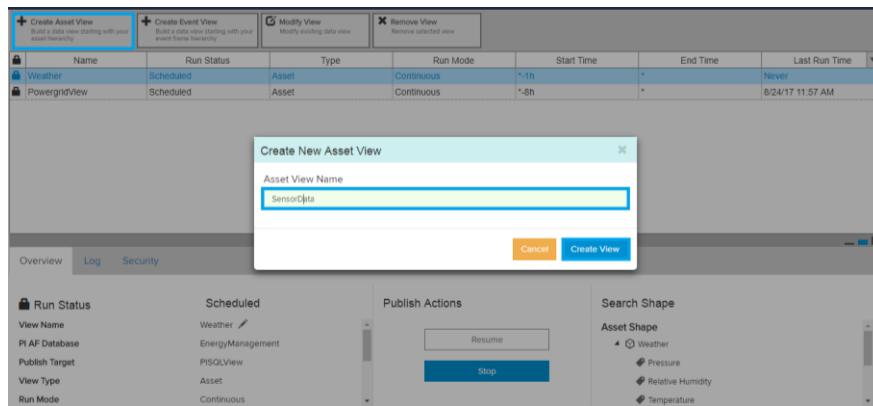
- Your Start Time is \*-1h
- Your End Time is \*
- Your Time Interval gets an interpolated measurement based on column Pressure

**Publish**

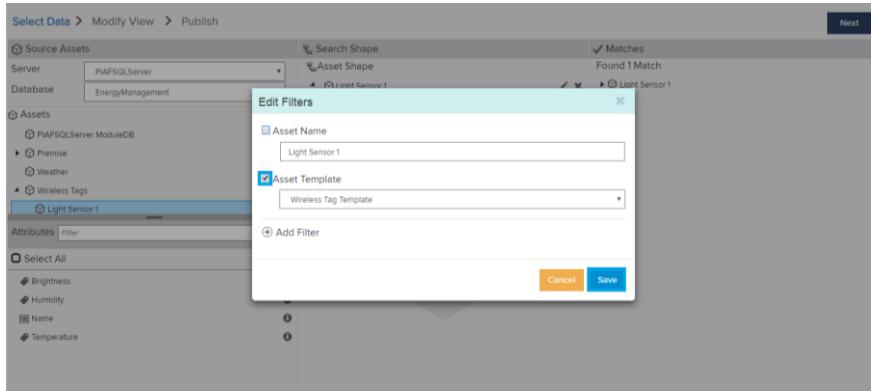
22. Click on **Confirm**.



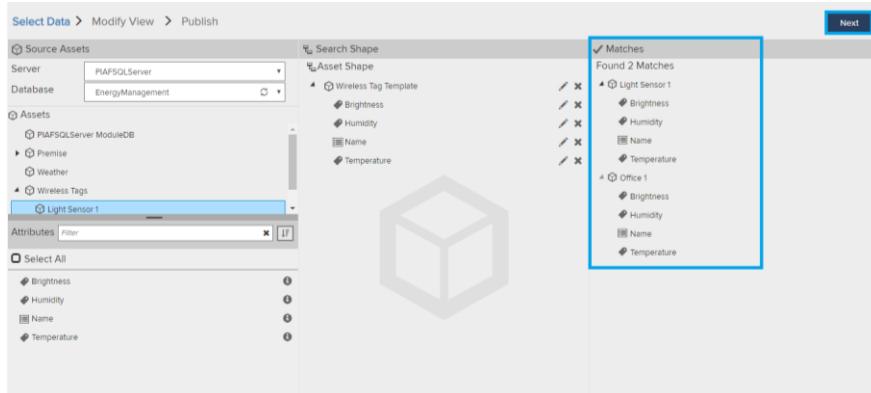
23. Create another Asset view with the name **SensorData** and click on **Create View**.



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**



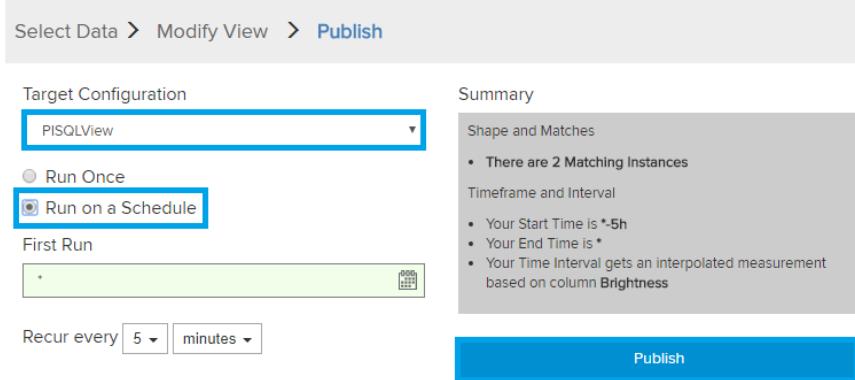
26. Click on **Edit Value Mode**, select **Use Key Column**, and **Save Changes**.

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

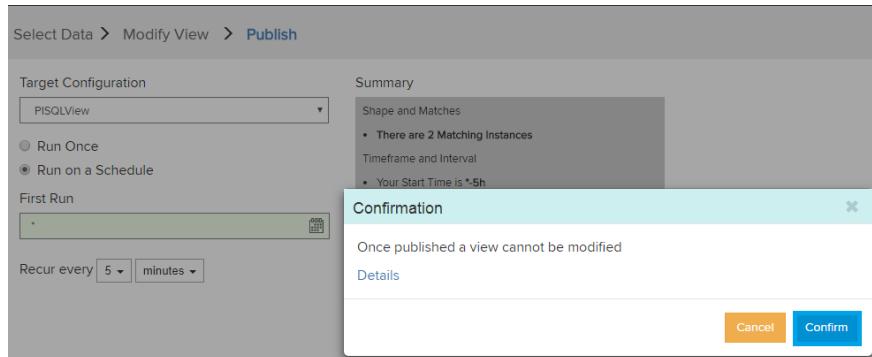
27. Select the start time as **\*-5h**, then click **Apply** and click **Next**.

Wireless Tag Template	TimeStamp	Brightness	Humidity	Name	Temperature
Office 1	8/24/2017 4:44:07.963 AM	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	2,277.261	48.417	Office 1	67.417
Office 1	8/24/2017 4:50:07.169 AM	318.511	30.856	Office 1	49.856
Office 1	8/24/2017 4:50:42.088 AM	923.605	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	50.401	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 4:54:41.616 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**.

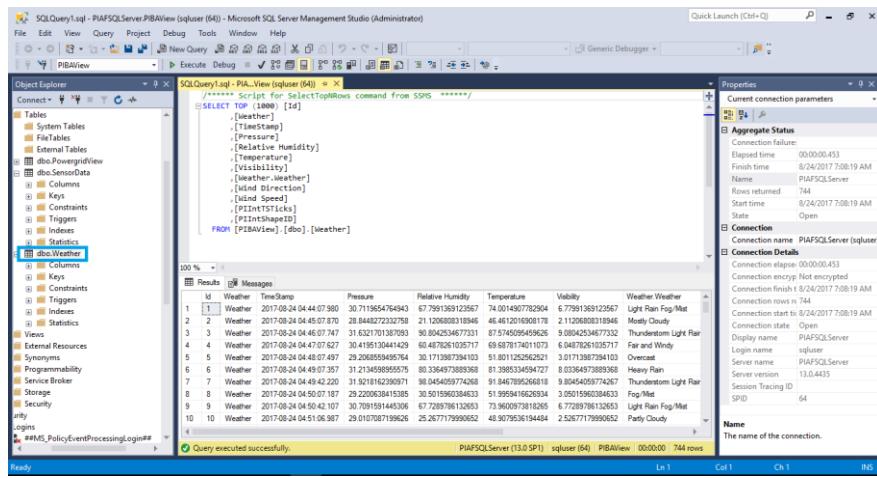


29. Click on **Confirm**.



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**.

**Commented [UD60]:** Make sure text and images are in sync



The screenshot shows the SQL Server Management Studio interface. In the Object Explorer, the 'Tables' node under the PIBAView database is expanded, showing the 'Weather' table. A query window titled 'SQLQuery1.sql - PIAFSQLServer.PIBAView (sqluser (64)) - Microsoft SQL Server Management Studio (Administrator)' contains the following T-SQL code:

```

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

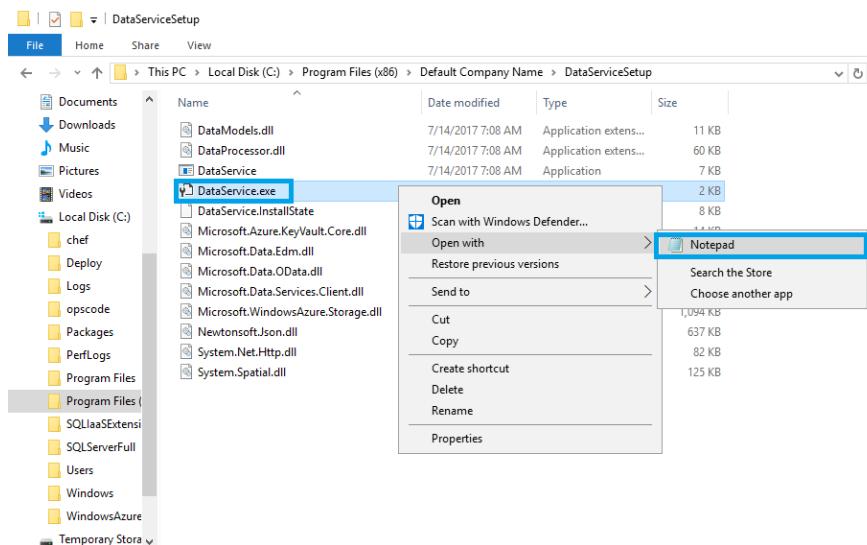
```

The results grid displays 1000 rows of weather data. The columns are: Id, Weather, TimeStamp, Pressure, Relative Humidity, Temperature, Visibility, Weather, Weather, Wind Direction, Wind Speed, PITIntSticks, and PITInShapeID. The first few rows of data are:

	M	Weather	TimeStamp	Pressure	Relative Humidity	Temperature	Visibility	Weather	Weather	Wind Direction	Wind Speed	PITIntSticks	PITInShapeID
1	1	Weather	2017-08-24 04:44:07.97	30.711954765493	67.799138912567	74.001400772954	6.7799138912567	Light Rain Fog/Mist	Light Rain Fog/Mist				
2	2	Weather	2017-08-24 04:45:07.87	28.044827232758	21.20080031894	46.412016080178	2.112060801894	Mostly Cloudy	Mostly Cloudy				
3	3	Weather	2017-08-24 04:46:07.747	31.623170138793	60.004253467733	87.674595469562	8.004253467733	Thunderstorm Light Rain	Fair and Windy				
4	4	Weather	2017-08-24 04:47:07.647	30.419530404129	60.4732610571	69.687174011078	6.04732610571	Fair and Windy	Fair and Windy				
5	5	Weather	2017-08-24 04:48:07.547	31.234678038343	60.4732610571	80.4732610571	6.04732610571	Overcast	Overcast				
6	6	Weather	2017-08-24 04:49:07.357	31.234678038348	81.398513454727	82.036497089368	8.1398513454727	Sunny Rain	Thunderstorm Light Rain				
7	7	Weather	2017-08-24 04:49:42.237	31.91816239071	90.045465974268	91.646795656118	9.045465974268	Fog/Mist	Fog/Mist				
8	8	Weather	2017-08-24 04:50:07.187	29.220053841585	30.501590324633	71.9600973812653	7.9600973812653	Light Rain Fog/Mist	Light Rain Fog/Mist				
9	9	Weather	2017-08-24 04:50:42.107	30.701591445058	72.288796132653	73.9600973812655	6.7288796132652	Partly Cloudy	Partly Cloudy				
10	10	Weather	2017-08-24 04:51:06.987	29.010787199626	25.267717990052	48.9079536194484	2.5267717990052						

The status bar at the bottom indicates: 'Query executed successfully.' and 'PIAFSQLServer (13.0 SP1) sqluser (64) PIBAView 00:00:00 744 rows'.

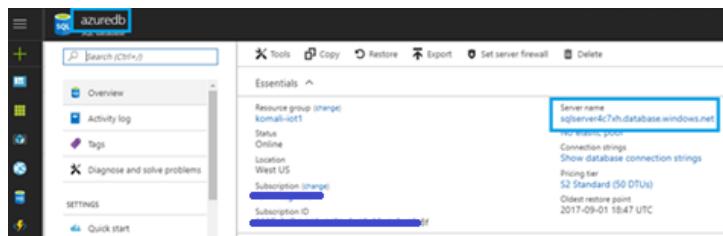
31. Navigate to **Local Disk (C:) > Program Files (\*86) > Default company name > Data Services Setup** > Right click on **Dataservice.exe**, then file open with notepad.



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**

Commented [AS61]: Azure SQL DB pass environment



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

Commented [AS62]: From do we get these values

Commented [SN63R62]: updated

NAME	TYPE	LOCATION	...
myjob4cxn	Scheduler Job Collection	West US	...
azuredb	SQL database	West US	...
dsm	SQL database	West US	...

The screenshot shows the 'Access keys' section of the Azure Storage blade. It displays two access keys: 'key1' and 'key2'. Each key has a 'NAME' field, a 'KEY' field containing a long hex string, and a 'CONNECTION STRING' field. The connection strings are identical, pointing to 'https://AccountName.webjobstr4c7vh.blob.core.windows.net/'.

**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.

```
<configuration>
<connectionStrings>
<add name="PIAServerConnectionString" value="Data Source=PIAServer;Initial Catalog=PIAView;Persist Security Info=True;User Id=sqliuser;Password=@1234" />
</connectionStrings>
<appSettings>
<add key="PIAServer" value="PIAServer" />
<add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=webjobstr4c7vh;AccountKey=n929qGah0ffJ3a08rXf0bMfrw/ISg/JFfaJNQnHfScK2" />
<add key="PIAServerConnectionString" value="Data Source=PIAServer;Initial Catalog=PIAView;Persist Security Info=True;User Id=sqliuser;Password=@1234" />
</appSettings>
<runtime>
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
<dependentAssembly>
<assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a5eed" culture="neutral" />
<bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
</dependentAssembly>
</assemblyBinding>
</runtime>
</configuration>
```

**Commented [AS64]:** Need to add the name of the db as it is hardcoded in ARM template.

**Commented [SN65R64]:** you have update new db that is "PIAView" which you created in af server to config pibavmserver

**Commented [AS66]:** From where do we get these values. Explain...

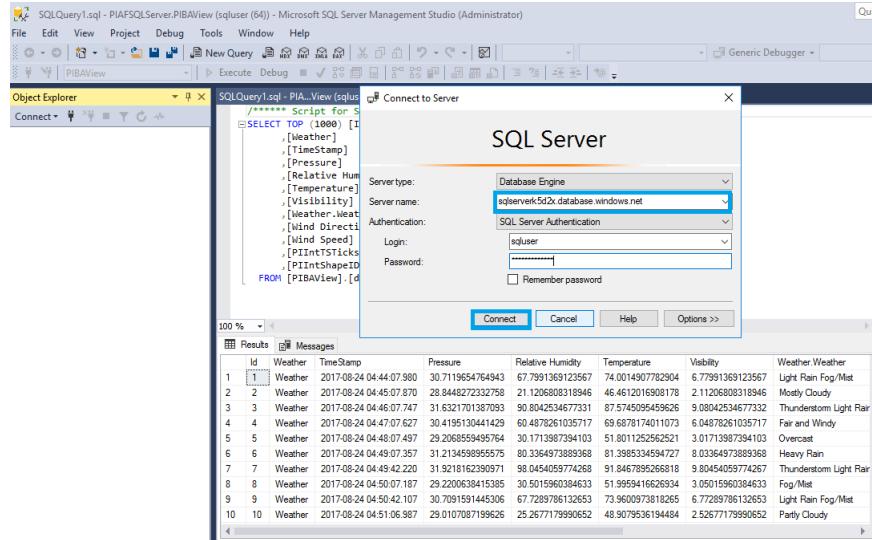
**Commented [SN67R66]:** follow 32nd point

**Commented [SN68R66]:** added screenshots from where we get values

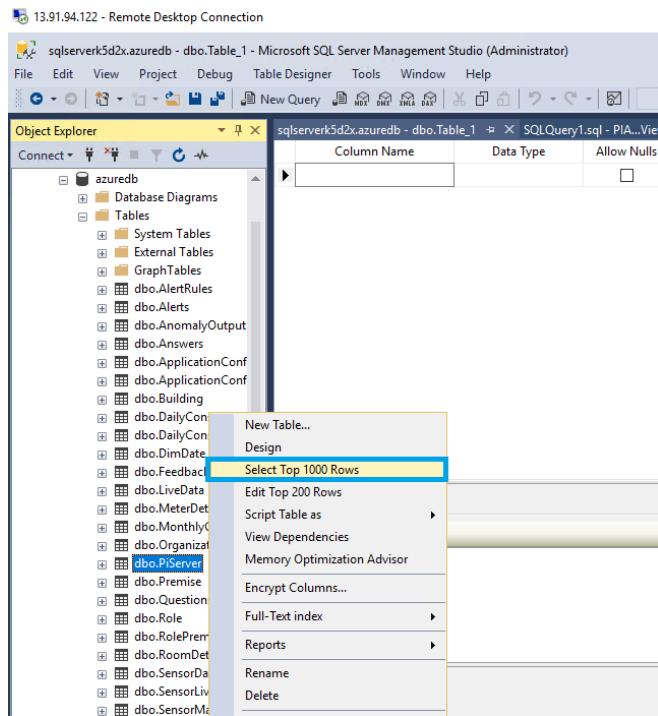
33. After updating the values in the data service.exe files, navigate **Start > Service** to start the DataServicesEM.

The screenshot shows the Windows Services window. The 'DataServiceEM' service is selected and its properties are displayed. The 'Status' is shown as 'Running' and the 'Startup Type' is 'Automatic'. A context menu is open over the service, with the 'Start' option highlighted. Other options visible in the menu include 'Stop', 'Pause', 'Resume', 'Restart', 'All Tasks', and 'Properties'.

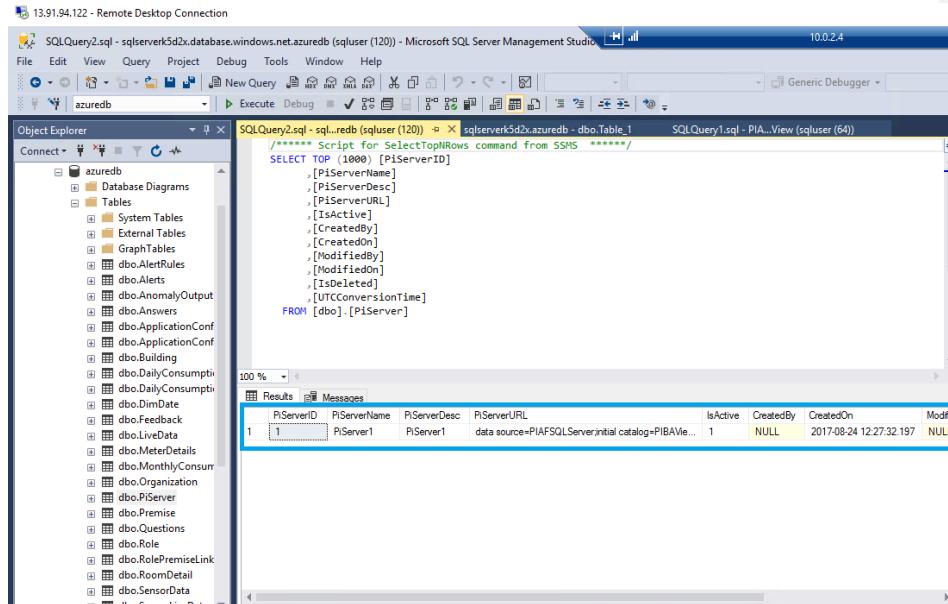
34. To check the data, we need to login to SQL server management studio in AF server with azure SQL server name with SQL login credentials and click on **connect**.



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



36. Check the updated table.

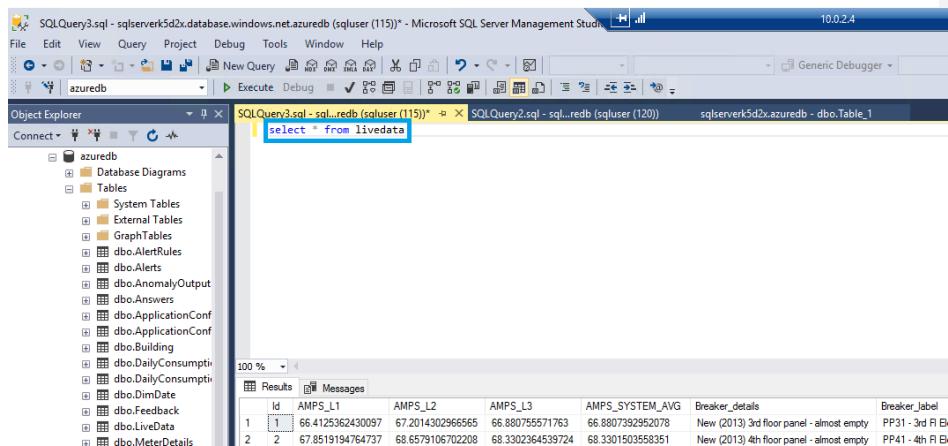


SQLQuery2.sql - sql-redb (sqluser (120)) - Microsoft SQL Server Management Studio 10.0.2.4

```
SELECT TOP (1000) [PIServerID]
      ,[PIServerName]
      ,[PIServerDesc]
      ,[PIServerURL]
      ,[IsActive]
      ,[CreatedBy]
      ,[CreatedOn]
      ,[ModifiedBy]
      ,[ModifiedOn]
      ,[IsDeleted]
      ,[UTCConversionTime]
  FROM [dbo].[PIServer]
```

The screenshot shows the Object Explorer on the left with the database 'azuredb' selected. The Results pane on the right displays the output of the above SQL query. The table has columns: PIServerID, PIServerName, PIServerDesc, PIServerURL, IsActive, CreatedBy, CreatedOn, and ModifiedOn. There is one row returned:

PIServerID	PIServerName	PIServerDesc	PIServerURL	IsActive	CreatedBy	CreatedOn	ModifiedOn
1	PIServer1	PIServer1	data source=PIAFSQLServer;initial catalog=PIAVie...	1	NULL	2017-08-24 12:27:32.197	NULL



SQLQuery3.sql - sql-redb (sqluser (115)) - Microsoft SQL Server Management Studio 10.0.2.4

```
select * from liveData
```

The screenshot shows the Object Explorer on the left with the database 'azuredb' selected. The Results pane on the right displays the output of the above SQL query. The table has columns: Id, AMPS\_L1, AMPS\_L2, AMPS\_L3, AMPS\_SYSTEM\_AVG, Breaker\_details, and Breaker\_Label. Two rows are returned:

Id	AMPS_L1	AMPS_L2	AMPS_L3	AMPS_SYSTEM_AVG	Breaker_details	Breaker_Label
1	66.4125362430097	67.2014302966565	66.880755571763	66.880739252078	New (2013) 3rd floor panel - almost empty	PP31 - 3rd Fl Bl
2	67.85194764737	68.6579106702208	68.3302364539724	68.3301503558351	New (2013) 4th floor panel - almost empty	PP41 - 4th Fl Bl

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

File Edit View Query Project Debug Tools Window Help

New Query MDX DAX XMLA XMLE DAX

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 (sqluser (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

New Query MDX DAX XMLA XMLE DAX

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

SQLQuery3.sql - sal...redb (sqluser (115))\* SQLQuery2.sql - sql...redb (sqluser (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

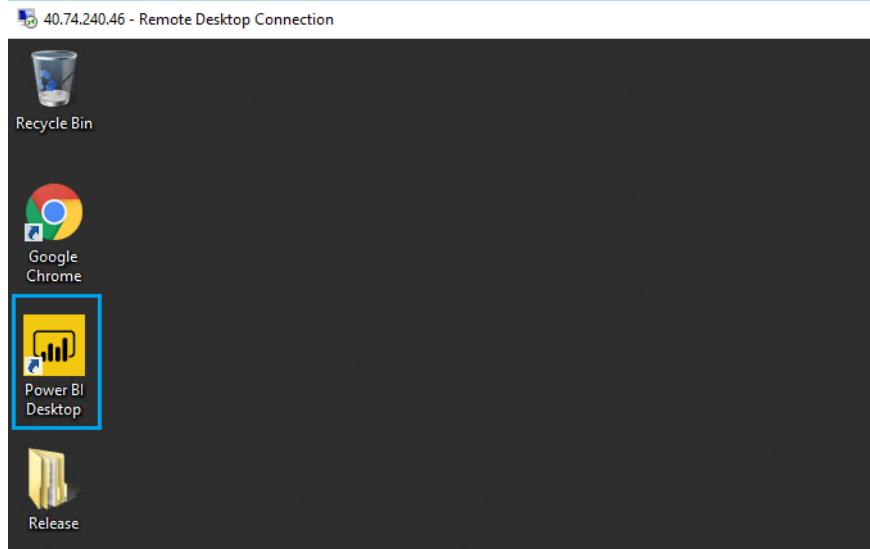
Connections from the IPs specified below provides access to all the databases in sqlserverk5d2x.

Allow access to Azure services **ON**

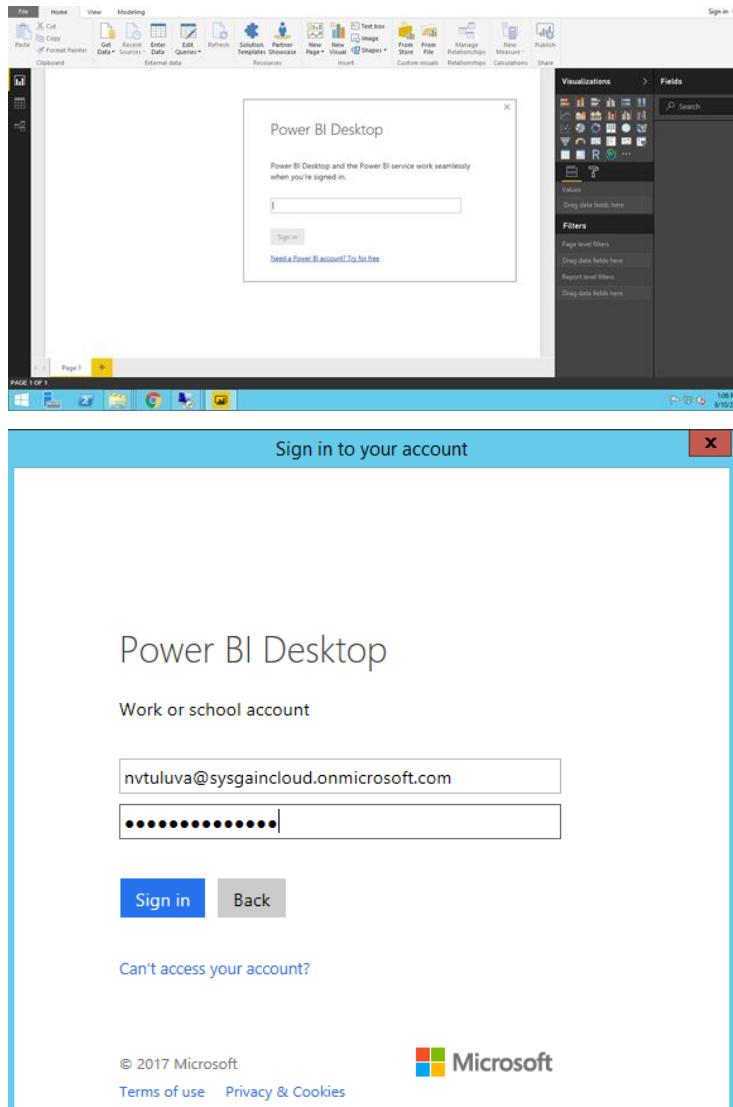
Client IP address 183.82.117.202

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

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



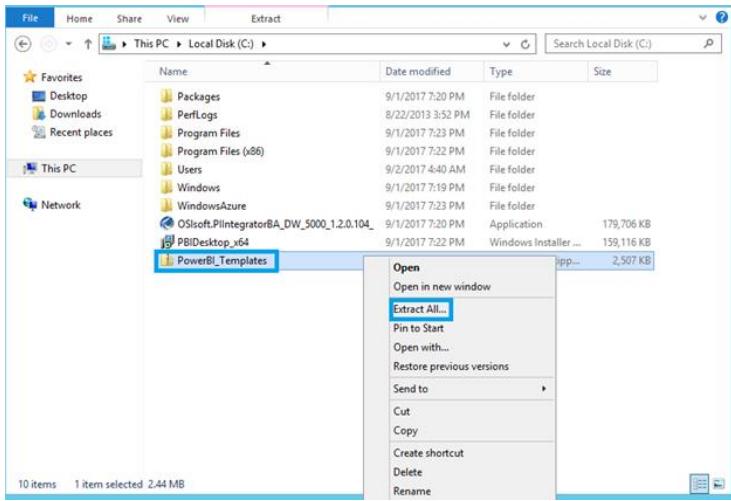
39. Log in with the same credentials used while registration of webapp with power BI you don't need to create a power BI account.



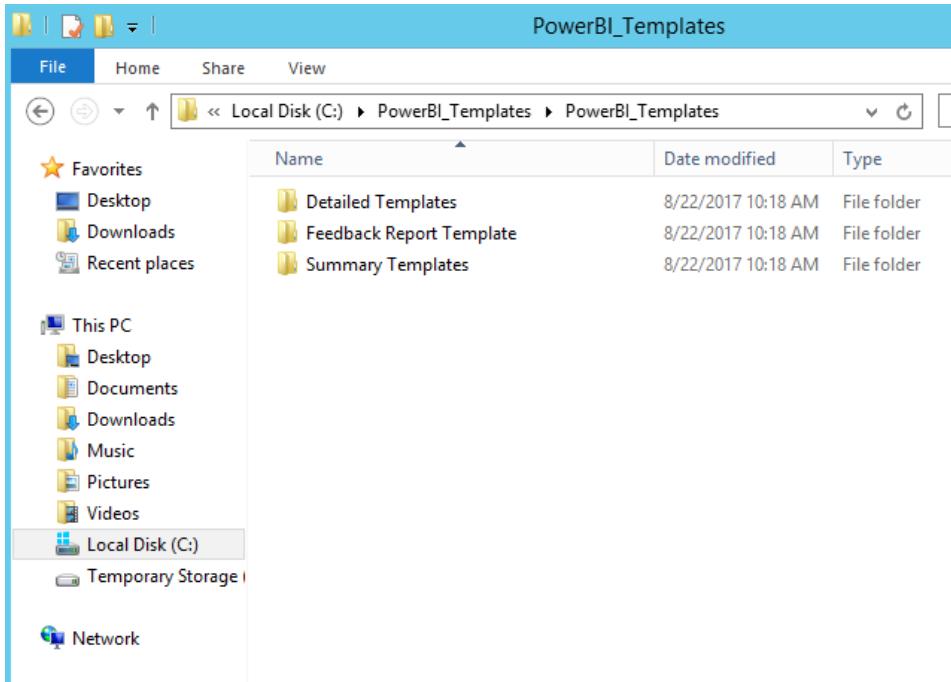
40. In Bastion server, navigate to **Local disk (C:) > unzip the Power Bi templates > Power Bi templates**.

**Commented [UD69]: Not clear**

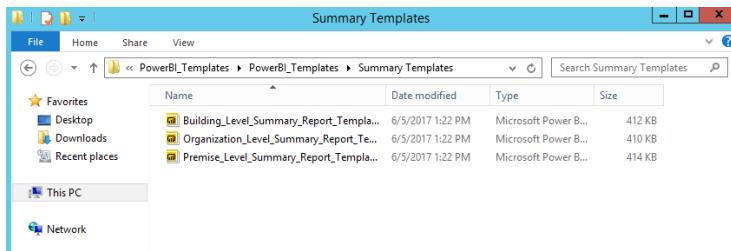
**Commented [KO70R69]: explained clearly pls check once**



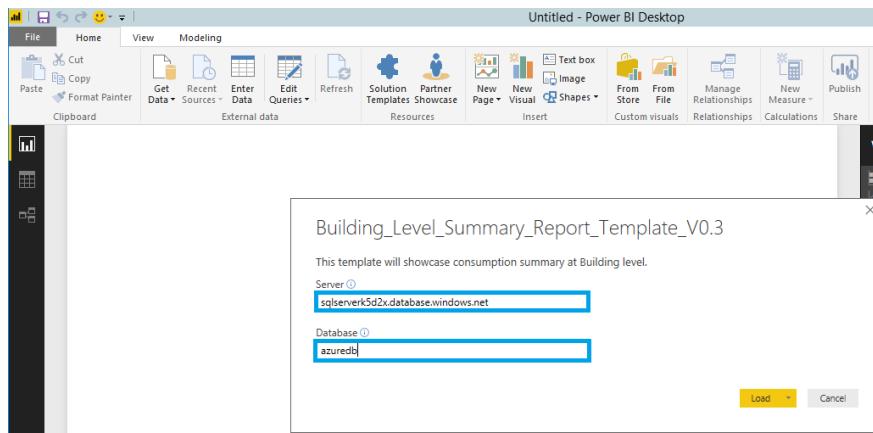
41. You can view Power Bi templates in the Local disk ( C : )



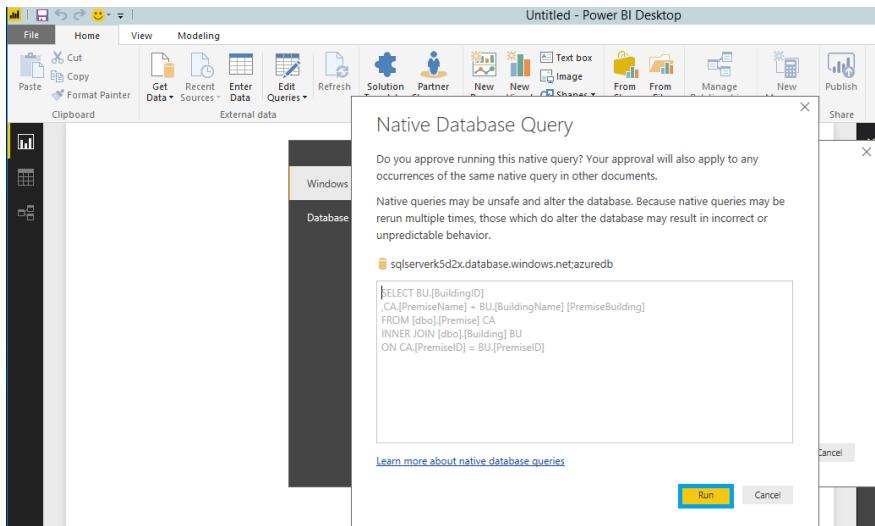
42. Navigate to the summary templates folder, click on "**Building\_level\_summary templates**" click on keep using Microsoft Power BI Desktop



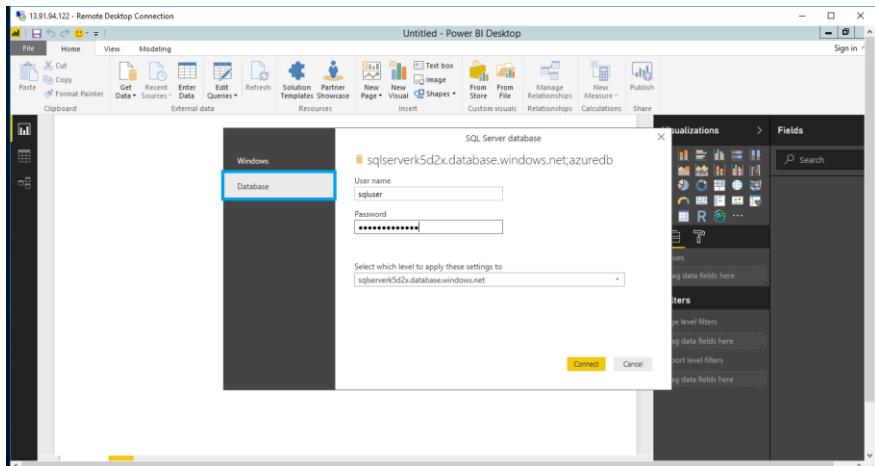
43. It prompts for power BI server and database details, provide you're Azure SQL server name and azure SQL database name from your deployed azure SQLServer .and click on **Load**.



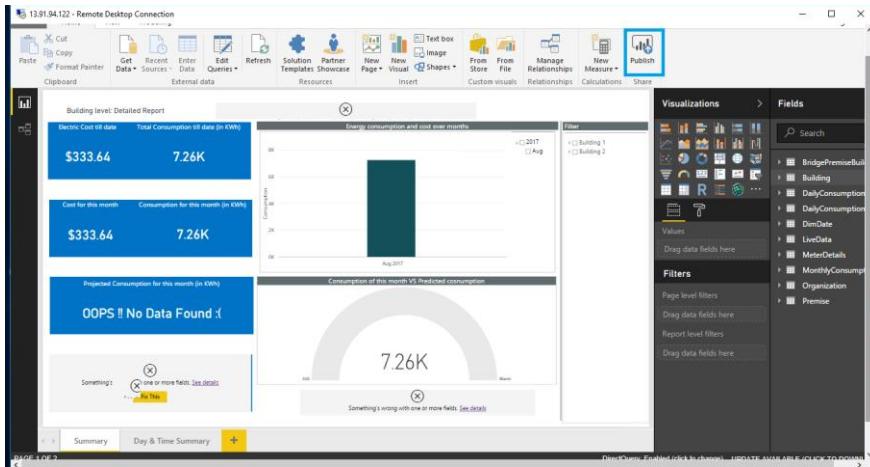
44. Once you click on Load , the "Native Database Query" will appear click on **Run**.



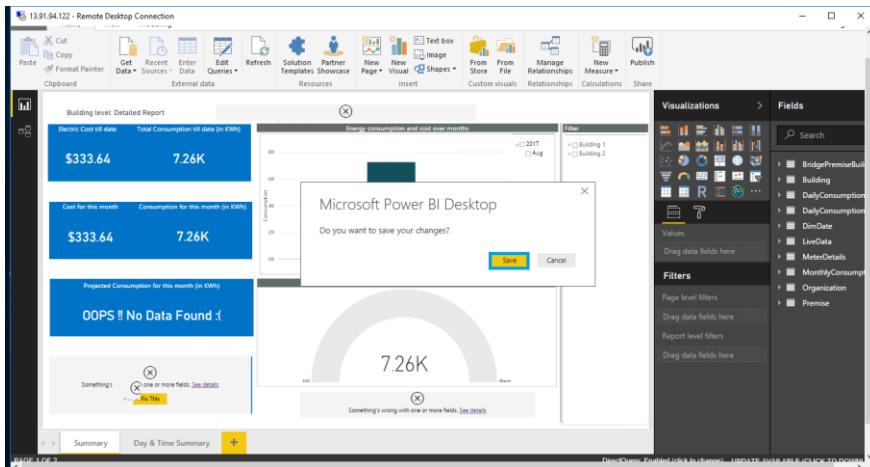
45. Select **Database** after connecting to the Azure SQL Server. Enter the login credentials of Azure database and click on **Connect**.



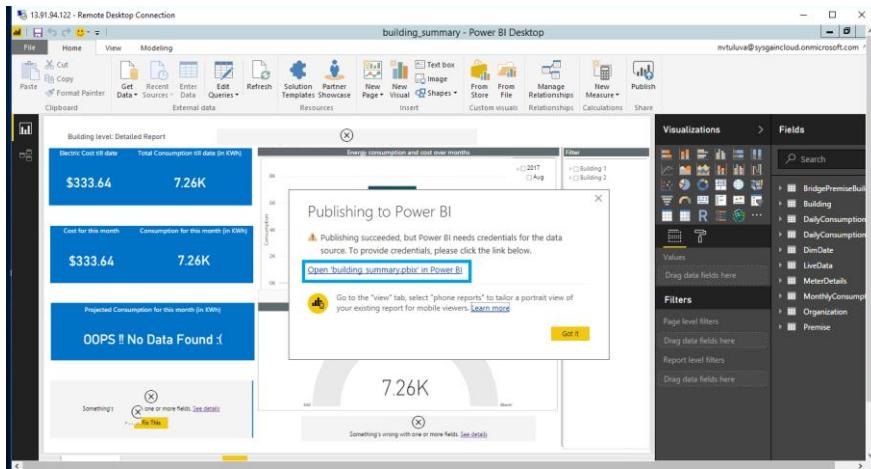
46. Click on **Publish**.



47. Save the changes.

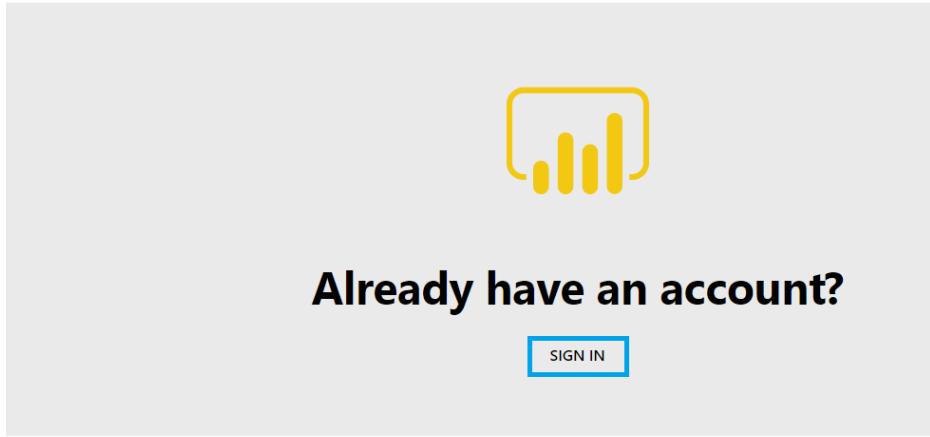


48. Click on the link as shown below, it will open in a web browser.

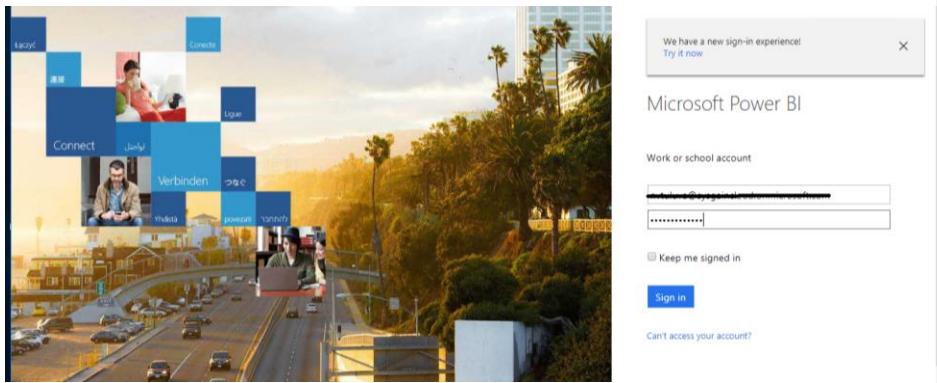


49. Sign in with the same credentials which were used to log to Power BI.

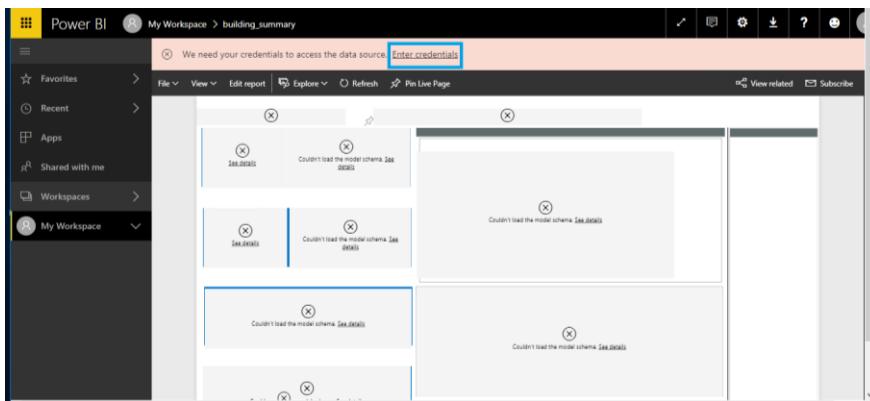
Microsoft | Power BI



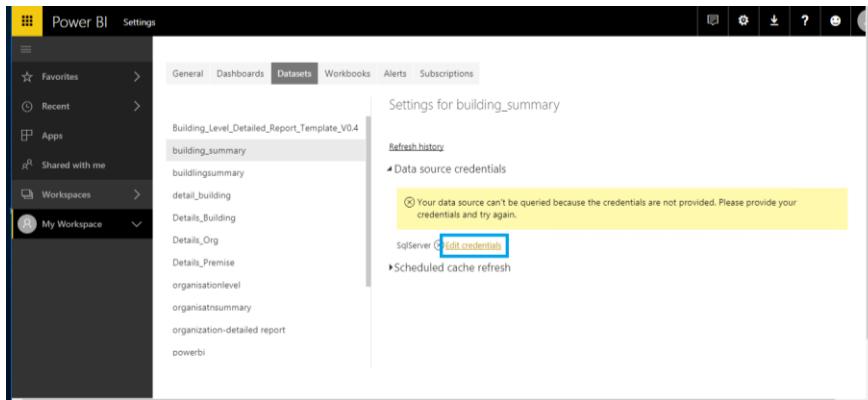
50. Enter the Power BI Credentials.



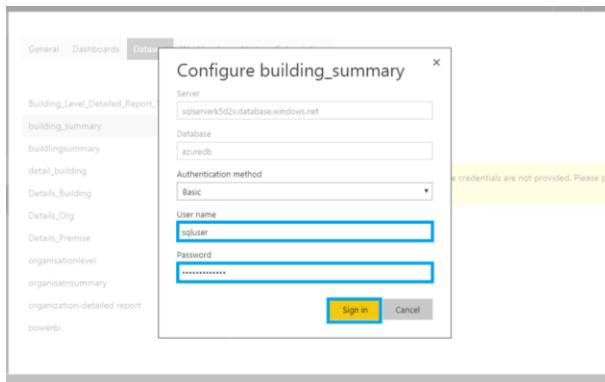
51. Click on **Enter credentials**.



52. Click on **Edit credentials**.



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



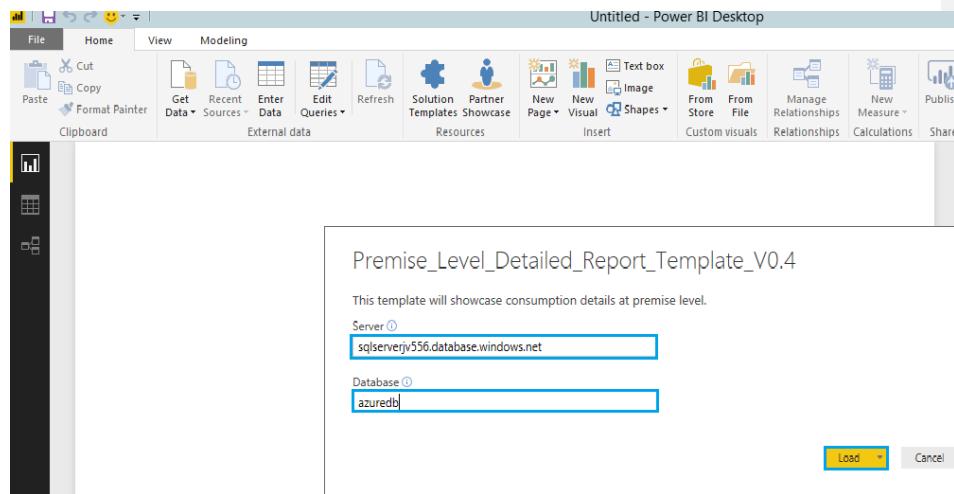
54. **Copy the token** from the URL publishing each template and **save it** for further configuration in web app.

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

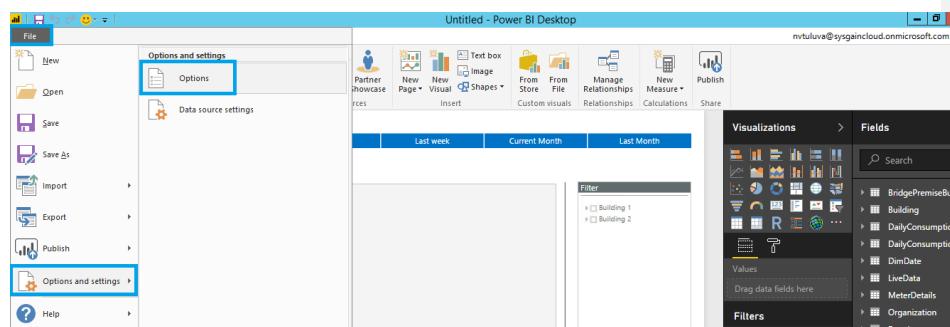
56. Navigate to **Power BI** templates and select **Detailed Template**.

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_Template...	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

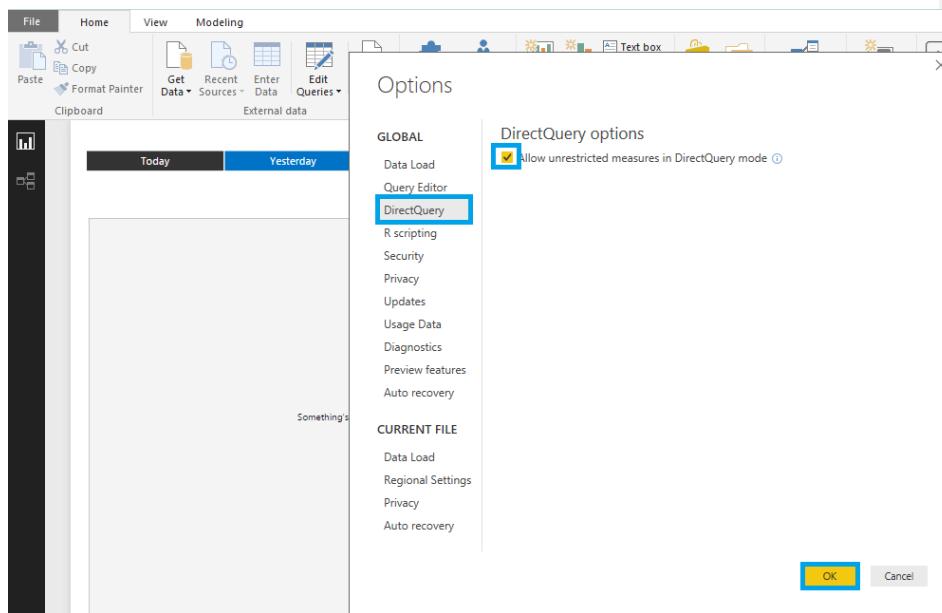
57. Enter the Azure SQL Server name with its password.



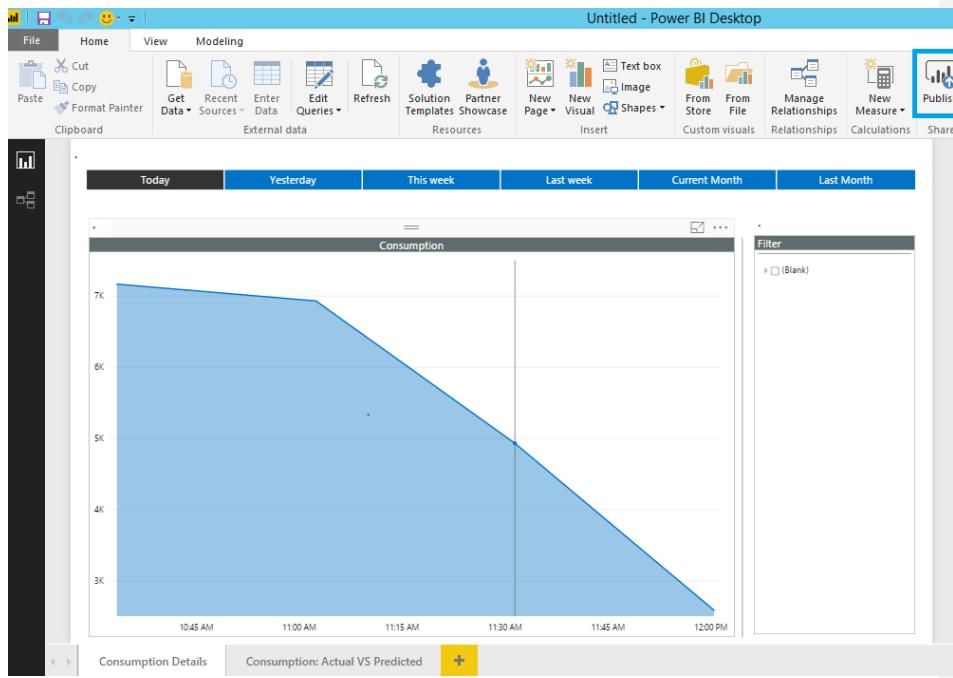
58. Navigate to **File > Options and Settings > Options**.



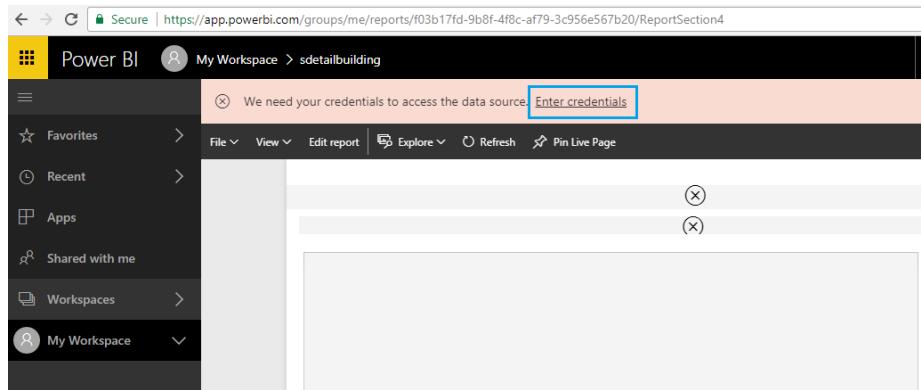
59. Select **DirectQuery** and then click on **OK**. Follow the same Process as done for the Summary template.



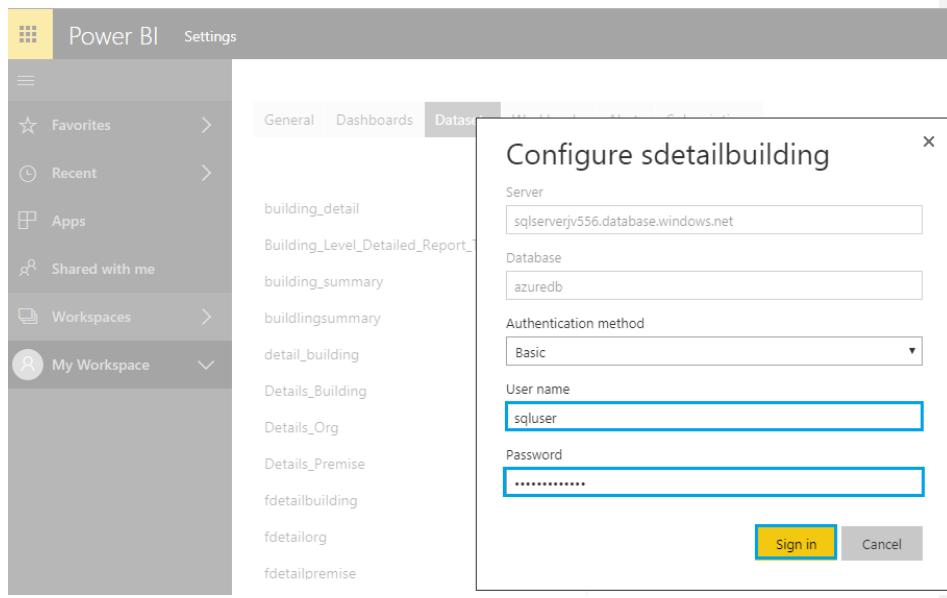
60. Click on **Publish** when you view the graph.



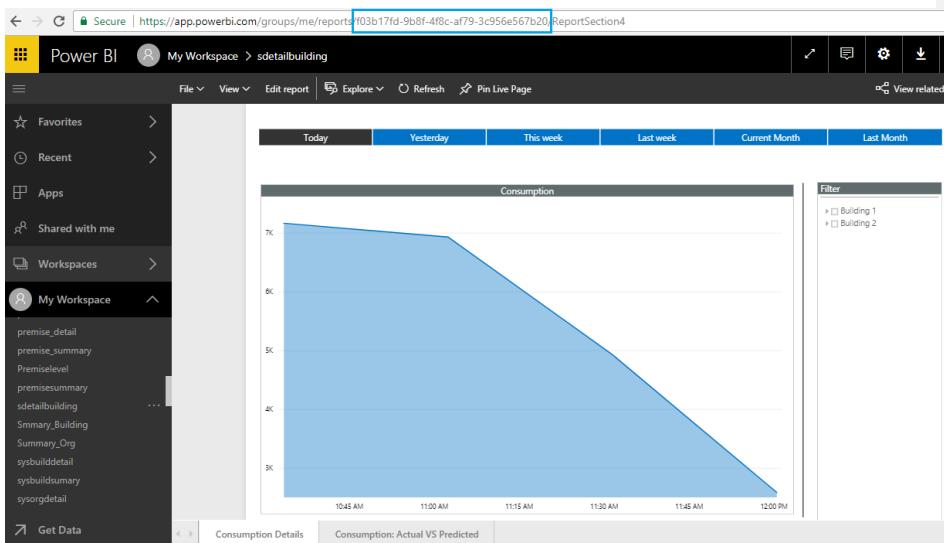
61. Click on **Enter credentials.**



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



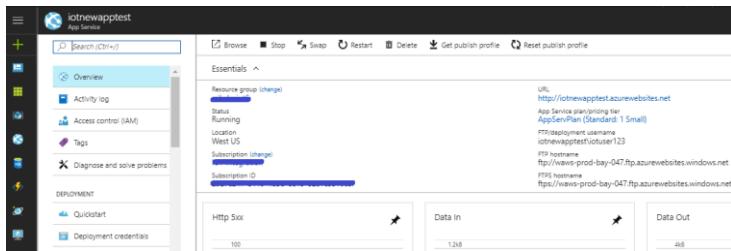
63. Copy the token from the URL after publishing each template and save it for further configuration in the web app.



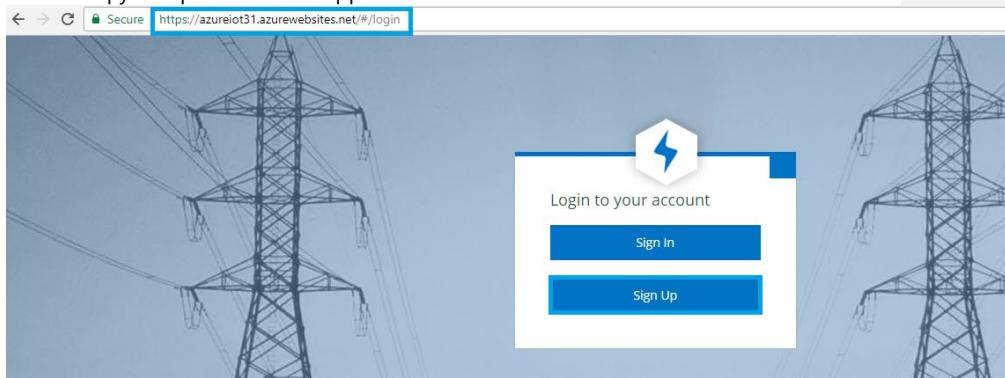
64. Repeat the same steps for organization and feedback detailed reports.

## 11. Configuring And Accessing The Webapp

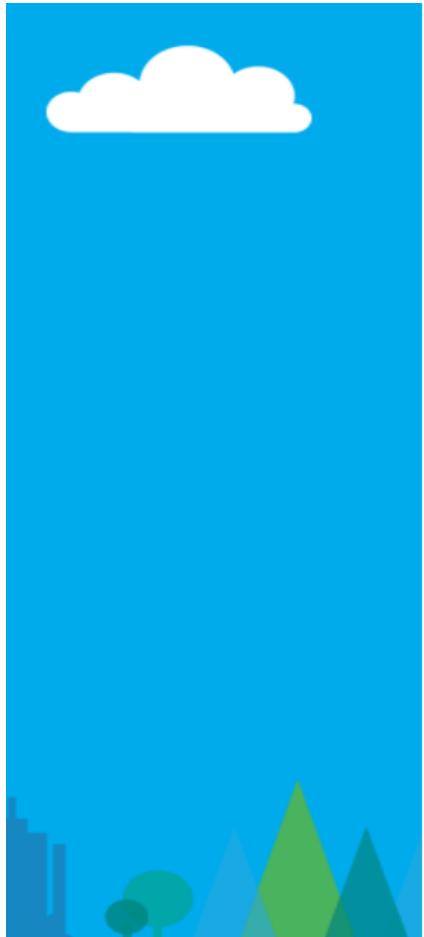
1. Go to the Web Application in the Resource Group and copy the "**URL**".



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

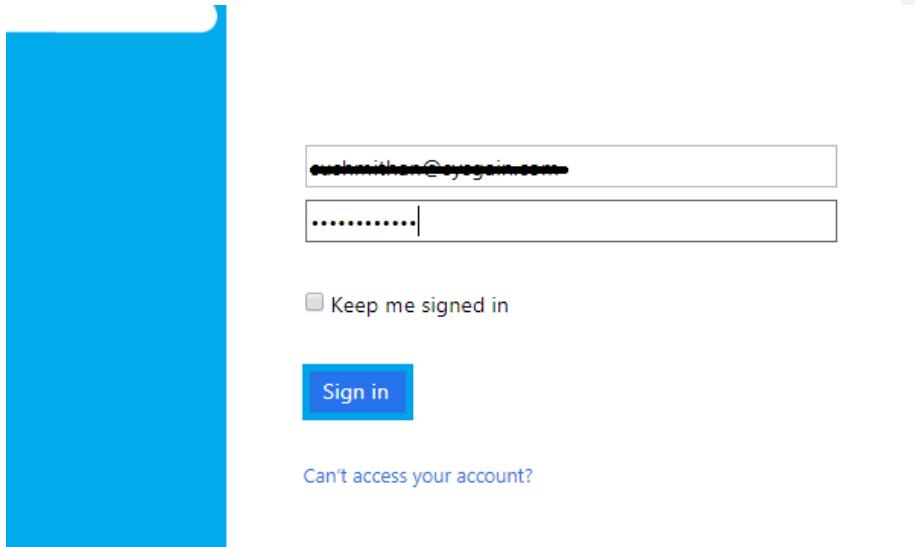
Display Name

Country/Region  
▼

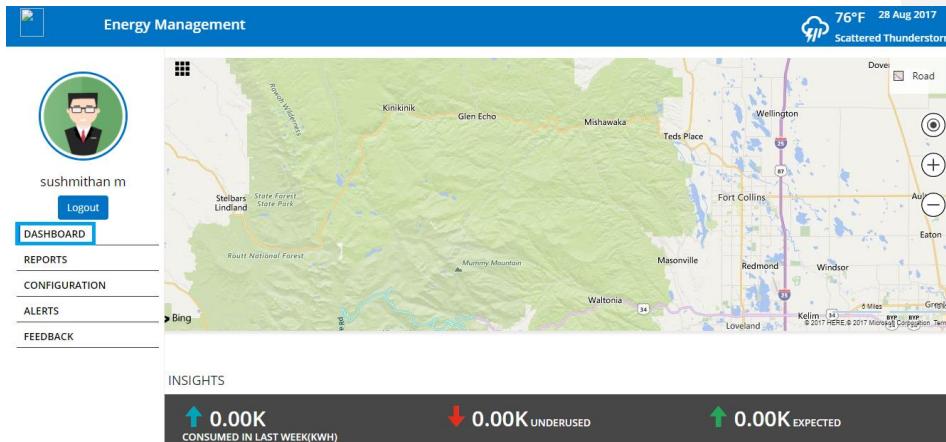
City

Activate Windows  
Visit [Windows Settings to activate Windows](#).

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



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



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

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

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

The screenshot shows the 'Energy Management' application interface. On the left, there is a sidebar with a user profile picture of a man with glasses and a suit, the name 'sushmithan m', and a 'Logout' button. Below the sidebar, the navigation menu includes 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted with a blue border), 'ALERTS', and 'FEEDBACK'. The main content area is titled 'Power BI Configuration(Organisation)' and contains two input fields with URLs: 'https://app.powerbi.com/reportEmbed?reportId=c440389c-e9db-4733-b541-fc1f4d08f116' and 'https://app.powerbi.com/reportEmbed?reportId=f03b17fd-9b8f-4f8c-af79-3c956e567b20'. There is also a red 'Power BI Configuration(Feedback)' bar at the bottom. A blue 'Add' button is located in the center of the configuration section.

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**.

This screenshot shows the same application interface as the previous one, but the configuration section has been expanded. It now includes three tabs: 'Power BI Configuration(Organisation)', 'Power BI Configuration(Premise)', and 'Power BI Configuration(Building)'. The 'Power BI Configuration(Premise)' tab is currently active, showing two input fields with URLs: 'https://app.powerbi.com/reportEmbed?reportId=48bbe94e-a82a-4cfb-820e-8e66c83c2501' and 'https://app.powerbi.com/reportEmbed?reportId=076c4c08-22c9-4e51-8c0a-13b10beb4695'. A blue 'Add' button is located in the center of the configuration section.

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 in a suit, the name 'sushmithan m', and a 'Logout' button. Below the sidebar are navigation links: 'DASHBOARD', 'REPORTS', 'CONFIGURATION' (which is highlighted with a blue border), and 'ALERTS'. The main content area has a blue header 'Power BI Configuration(Premise)'. Below the header, there are two URLs in blue boxes: 'https://app.powerbi.com/reportEmbed?reportId=935e322c-3719-4bad-97df-e8b5ca39761a' and 'https://app.powerbi.com/reportEmbed?reportId=75f040bd-d964-4510-9684-cc2f46a46999'. At the bottom right of this section is a blue 'Add' button. Below this section is another red box labeled 'Power BI Configuration(Building)'.

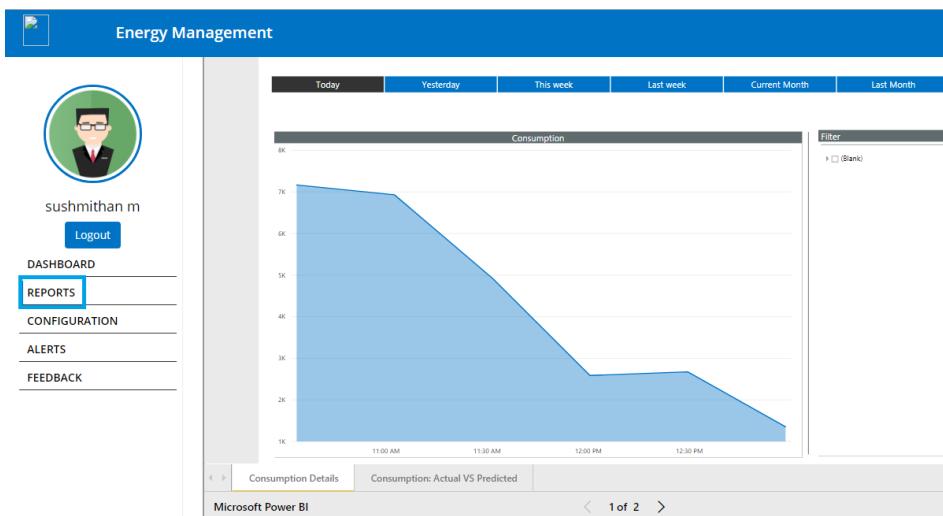
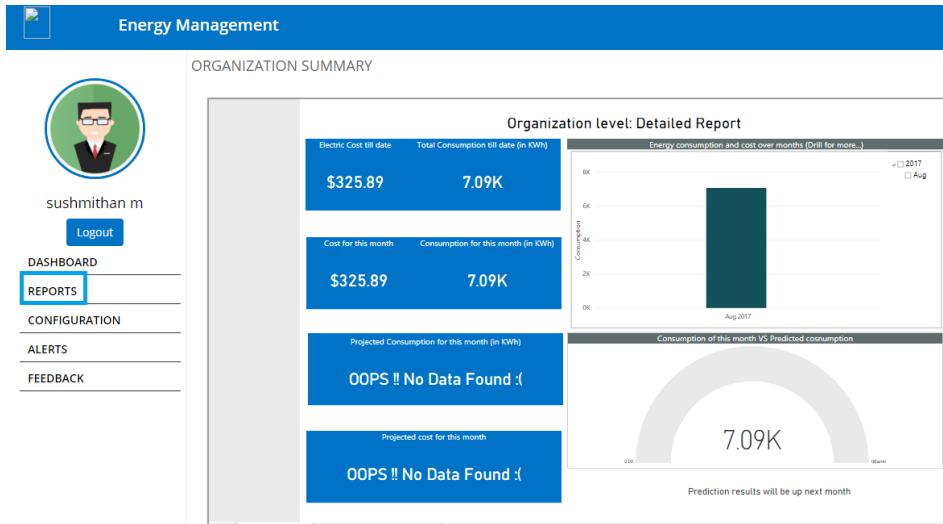
9. Enter the details of the Power BI which were used to register the **Power BI** with the web app and the **client id** and **client secret** which we got after resetting the app. Click on **Add**.

This screenshot shows the same 'Energy Management' application interface as the previous one. The sidebar and navigation links are identical. The main content area now has a blue header 'Power BI Credentials'. Below the header, there are four red boxes containing sensitive information: '4722d592-4fac-41f3-91c1-04e17238ca40', 'bQRuiQQUhrZMKWHeLwsjeVTFj/zOOAty6rAdKbUTtI8=', and two other obscured lines. At the bottom right of this section is a blue 'Add' button.

Commented [UD71]: Strike or blur all the creds

Commented [KO72R71]: updated

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

Microsoft Azure - Resource groups > Overview

Subscription name (changed) Deployments  
IOT Integration 12 Succeeded

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
AnureBackup_ndServer	Microsoft.Compute/resto...	South Central US
AzureBackup_bastionServer	Microsoft.Compute/resto...	South Central US

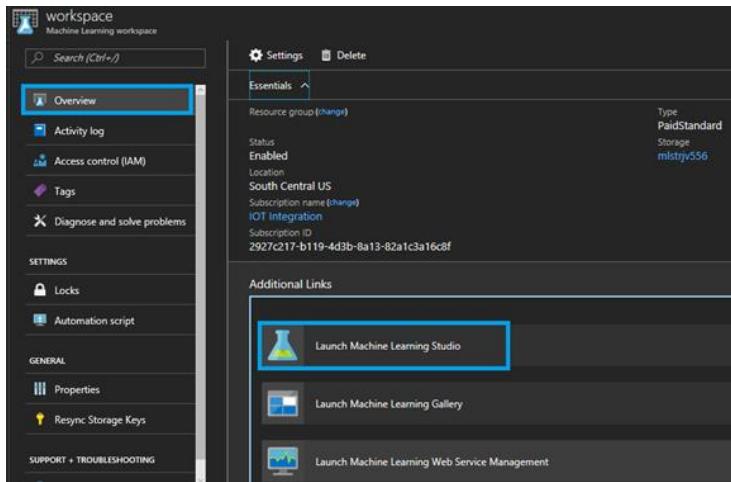
2. Click on the **workspace**.

Microsoft Azure - Resource groups > Overview

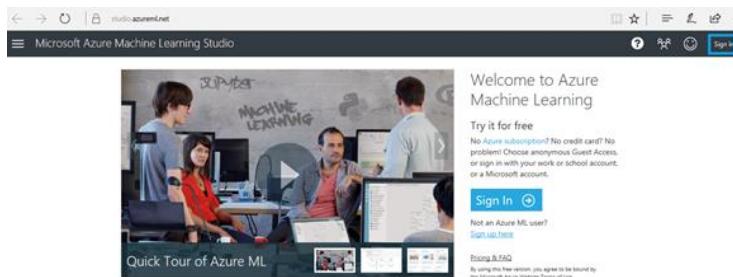
Subscription name (changed) Deployments  
IOT Integration 12 Succeeded

NAME	TYPE	LOCATION
splunkserver_disk2_b77ad535b934e699fe...	Disk	South Central US
splunkserver_OsDisk_1_d6289ffaa4d425e8e...	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**.



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



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>

A screenshot of a web browser displaying the Cortana Intelligence Gallery. The page shows an experiment titled "ERM\_Experiment\_1 [Predictive Exp.]". It includes a summary, a description mentioning "The following Predictive experiment helps in ways to minimize the Power Utilization costs", and a preview image of a data flow diagram. Buttons for "Open in Studio" and "Add to Collection" are visible.

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

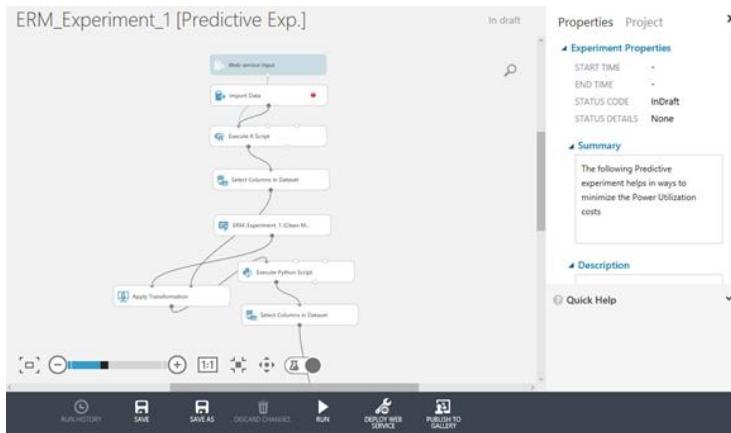
## Copy experiment from Gallery

REGION:

WORKSPACE:

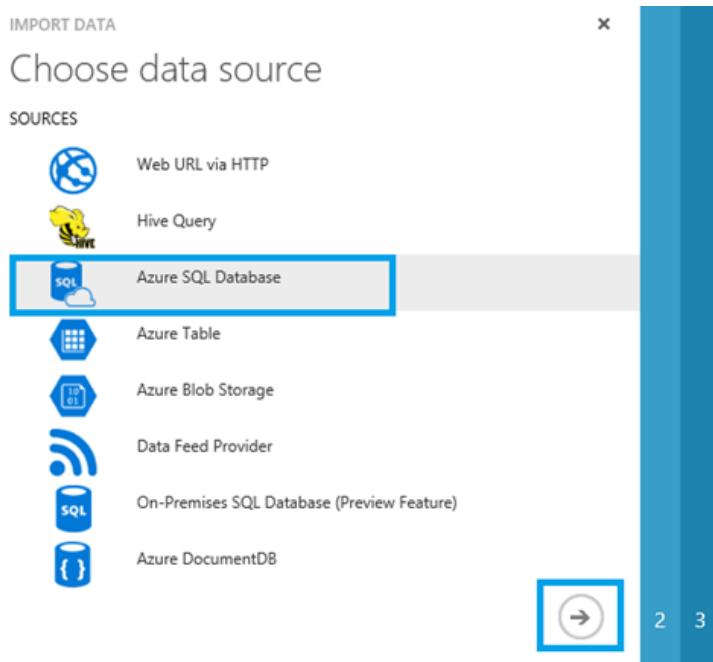


7. The experiment gets downloaded in our workspace.

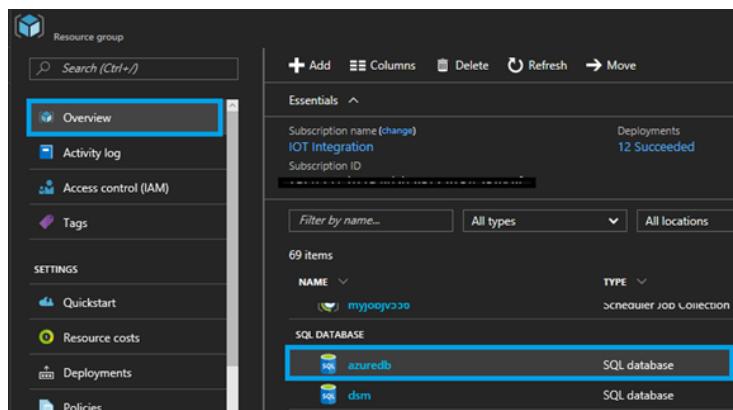


8. Once the experiment got pulled in the workspace, click on **Import Data**. Now click on **Launch Import Data Wizard** from right side menu.

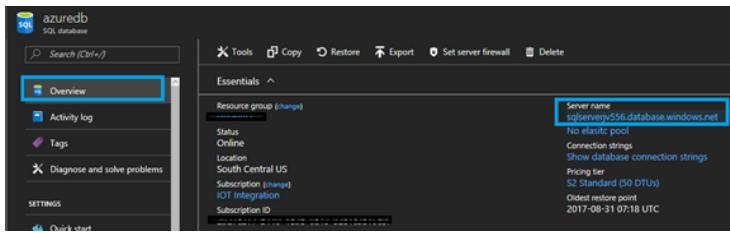
9. Select **Azure SQL Database** and click on Next icon “->”.



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



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



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

Enter the **Database name**, **User name** and **Password** 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

\*\*\*\*\*

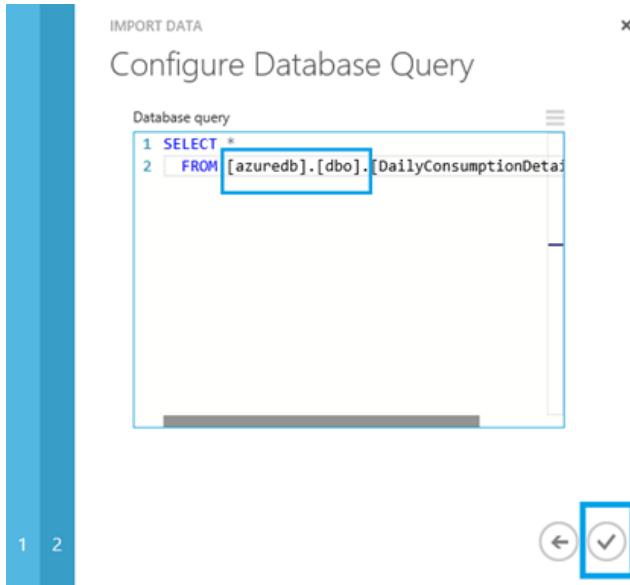
Accept any server certificate (insecure)

**Test Connection**

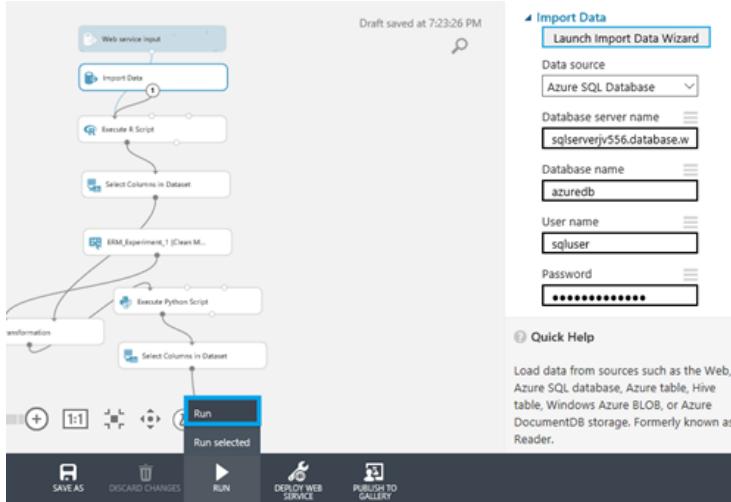
Test connection succeeded.

← →

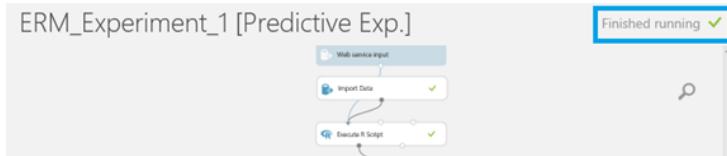
13. Replace the Database name with **azuredb** and click on **tick mark**.



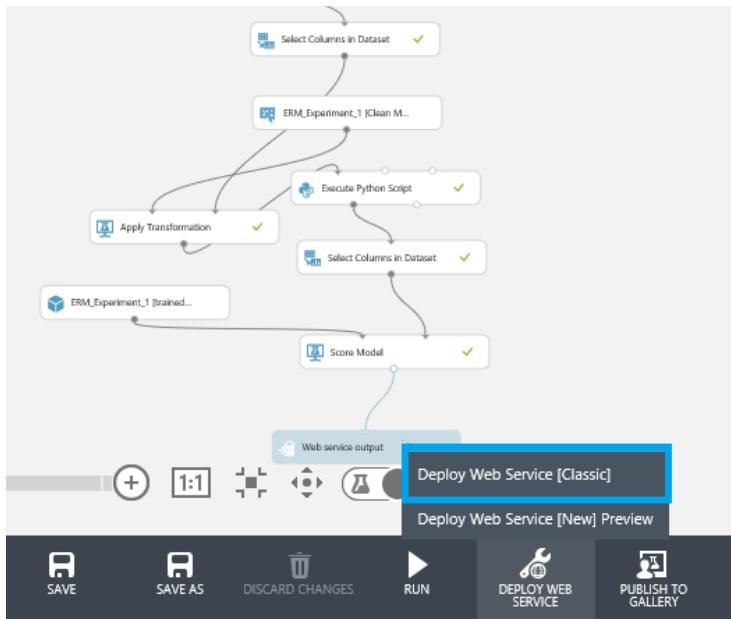
14. Once done run the experiment by right clicking on **Run** from bottom of the below screen and from the appeared menu click on **Run**.



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

```
+n92PDuzx70O/tptyGUURfls0U0AaCgbgmhZ03PjCxoiWwww4J0Q7+tDaUEMESBIDFwxzgVbB+aOP0Lh5sag==
```

Default Endpoint

API HELP PAGE TEST APPS

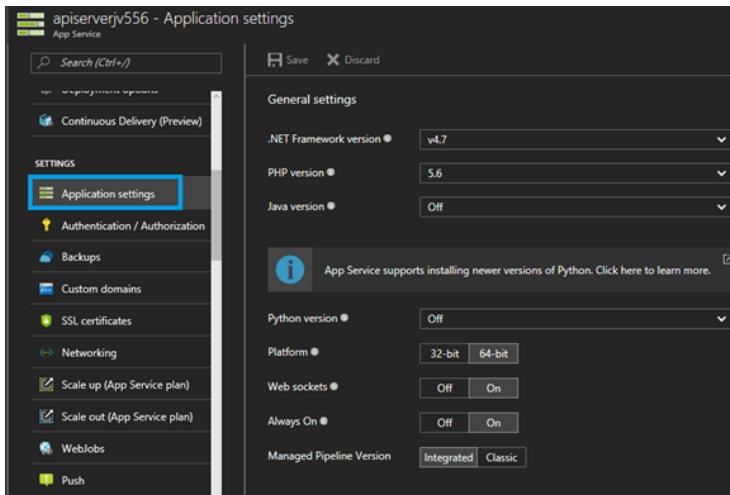
REQUEST/RESPONSE Test Test preview Excel 2013 or later |  
Test preview Excel 2013 or later |

BATCH EXECUTION

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	
<b>Application settings</b>	
Authentication / Authorization	
Backups	
Custom domains	
SSL certificates	
Networking	
Scale up (App Service plan)	
Scale out (App Service plan)	
WebJobs	
Push	

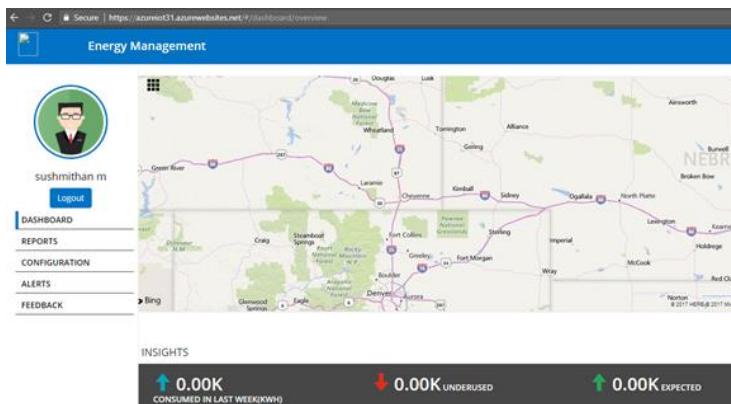
  

b2cSignInPolicyId	B2C_1_simplerPolicy2
b2cClientSecret	390KSgOLN\$rf7
b2cChangePasswordPolicy	B2C_1_cpasswordpolicy
EmailHost	iothost
EmailHostPort	25
EmailSender	noreply@gmail.com
EmailHostPassword	Password@1234
BlobStorageConnectionString	DefaultEndpointsProtocol=https;AccountName=webjo...
AzureMIAnomalyDetectionApiKey	+n92PDuxz700/tpusyGUKRfls0Uf0AaCgbgmhZ039jCxi...
AzureMIAnomalyDetectionApiUrl	https://ussouthcentral.services.azureml.net/workspaces/...

21. Restart the **apiserver**.

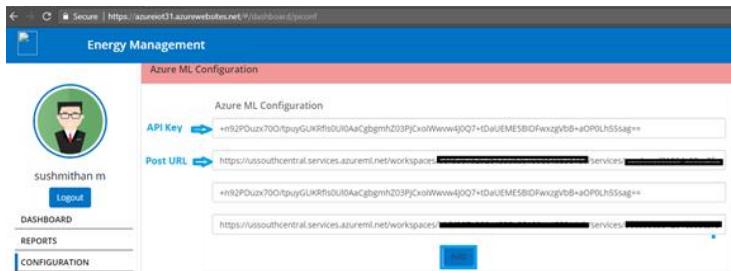
SETTINGS	
<b>Application settings</b>	
Authentication / Authorization	b2cSignInPolicyId B2C_1_sinpolicy2
Backups	b2cClientSecret 390K5g0JN5rlf7
Custom domains	b2cChangePasswordPolicy B2C_1_cpasspolicy
SSL certificates	EmailHost iothost
Networking	EmailHostPort 25
Scale up (App Service plan)	EmailSender noreply@gmail.com
Scale out (App Service plan)	EmailHostPassword Password@1234
WebJobs	BlobStorageConnectionString DefaultEndpointsProtocol=https;AccountName=webjo...
	AzureMLAnomalyDetectionApiKey +n92PDuzx70O/tputGUKRfsQIJ0AaCgbgmhZ03PjXoi...
	AzureMLAnomalyDetectionApiUrl https://ussouthcentral.services.azureml.net/workspaces/...

22. Login to the web application.

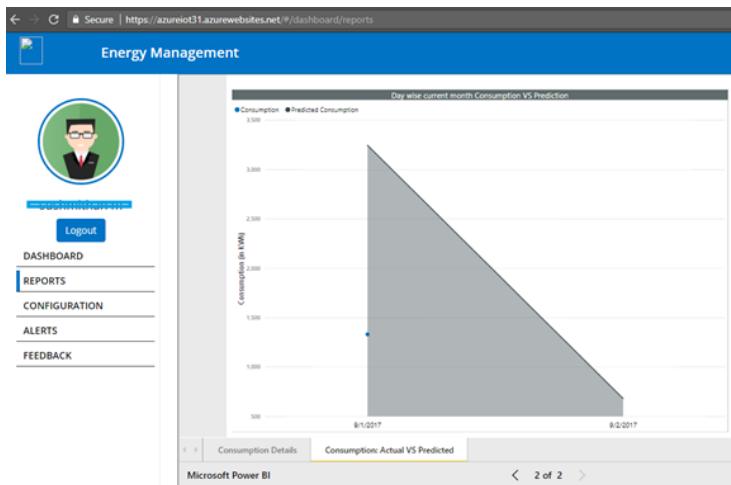


23. Navigate to **Azure ML Configuration** and add the **API Key** and **POST URL**.

Click on **Add**.

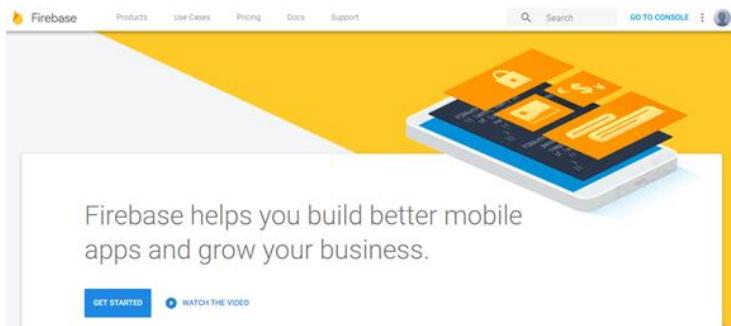


24. Click on **REPORTS** and click on **Consumption: Actual VS Predicted** of the bottom of the screen to view the Actual Vs Predicted graph.

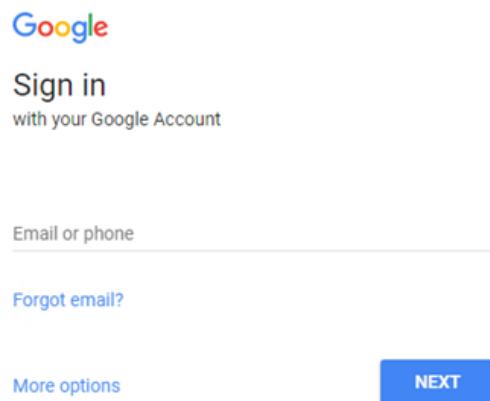


## 13. Firebase Configuration

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

Project name

Project ID ⓘ

iotproject-7fb4a

Country/region ⓘ

United States

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

By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable [terms](#).

CANCEL 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: **iotproject**

Project ID: **iotproject-7fb4a**

Country/region: **United States**

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

By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable [terms](#).

**CANCEL** **CREATE PROJECT**

<https://console.firebaseio.google.com/project/iotproject-7fb4a/settings/cloudmessaging/>

**Firebase** **iotproject**

**Settings** GENERAL CLOUD MESSAGING ANALYTICS ACCOUNT LINKING SERVICE ACCOUNTS

**Project credentials**

Key	Token
Server key	AAAA_0VZ0M...9t9vLw...4C2B7D...27Wz...P...4...E27...9tT1TaK...N...9tC72P...6...Ap...G...M...v...5...m...1...0...8...U...D...J...y...d...9...4...C...n...7...u...k...3...
Legacy server key	Az...0...n...7...7...d...a...l...0...J...P...P...P...e..._0...X...9...A...m...A...p...g...U...
Sender ID	1096487325347

**ADD SERVER KEY**

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

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

```

<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
  // Initialize Firebase
  var config = {
    apiKey: "AlzaSyAbTdFA76Xo5THJRqlRWLfdDn63uYGHlo8",
    authDomain: "iotproject-7fb4a.firebaseio.com",
    databaseURL: "https://iotproject-7fb4a.firebaseio.com",
    projectId: "iotproject-7fb4a",
    storageBucket: "iotproject-7fb4a.appspot.com",
    messagingSenderId: "1096497225347"
  };
  firebase.initializeApp(config);
</script>

```

```

<script src="https://www.gstatic.com/firebasejs/4.3.0.firebaseio.js"></script>
<script>
  // Initialize Firebase
  var config = {
    apiKey: "AlzaSyAbTdFA76Xo5THJRqlRWLfdDn63uYGHlo8",
    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>

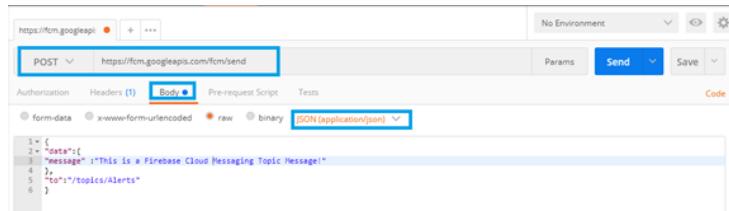
- Click on Body and enter the content

```

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

```

- Select the text to **Json**



- 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**.

- 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**

