InfoBurst installation guide (specific for azubw18005)

Compatibility/Requirements

The following matrix details the InfoBurst supported environments that we used to install and configure InfoBurst and connect to azubw18005 through InfoBurst.

Item	Version used (for **azubw18005**)
Windows Server	**Windows Server 2016 Datacenter**
Microsoft .NET Framework	**4.8 (installed automatically by InfoBurst installer)**
Power BI Service	**13.0.25310.47 (Version)**
SharePoint	**Sharepoint 2010-2018**
Web Browser	**InfoBurst requires an HTML5-compliant browser**

Windows Server

InfoBurst is a Microsoft .NET application and requires Windows Server and the Microsoft .NET Framework.

In the case of azubw18005, the server used is the Windows Server 2016 Datacenter and the operating system is Windows.

Hardware

The following are minimum hardware requirements for InfoBurst operation:

CPU	**16 vcpus**
Memory	**64 GiB memory**
Disk	**OS Disk:** **azubw18005_OsDisk_1_68d6a75ef2a04e3ca494410cd8a50ac6** **Storage Type**: Premium SSD LRS, Size (GiB): 127, Max IOPS: 500, Max throughput: 100, Encryption: SSE with PMK **Data Disk:** **azubw18005_DataDisk_0** **Storage Type**: Premium SSD LRS, Size (GiB): 128, Max IOPS: 500, Max throughput: 100, Encryption: SSE with PMK

Ports

We used InfoBurst port **8554** to perform our operations and tasks.

Database Repository

InfoBurst requires a database to host its repository. It uses SQLite as the repository type and **IBRepo.db** as the repository database. The SQLite database is created automatically upon installation.

SharePoint

We are using SharePoint 2010-2018 located on BI@ST dev (https://stmicroelectronics.sharepoint.com/teams/Bist). We particularly use the folders in the Infoburst folder section as the destination of our bursts.

Power BI Service

We are using Power BI Pro **13.0.25310.47 (Version)** provided with the ST subscription on beST. We are using the OAuth method of authentication to configure it. The detailed steps are given in the Power BI Access section.

Installation steps

- Ensure that the requirements given above are fulfilled
- Download the InfoBurst installer to the server
- Install the current version. Patches can only be issued for the current version.

Installation

- Right-click the installation file and select **Run as administrator** (if applicable)
- Select **Next** on the **Prerequisites Setup Wizard** to install the required Microsoft .NET Framework (if applicable). .NET Framework installation may require a server restart.
- Select **Next** on **InfoBurst Setup Wizard** Screen

- Select **I accept the terms of the License Agreement** then select **Next**

- Select **Next** to install in default folder. Select **Change** to install in directory other than default, then select **Next.**

- **Windows Service Credentials:** Enter a Windows administrator account to run the InfoBurst service. Right click on the application and click on "**Run as Administrator**".

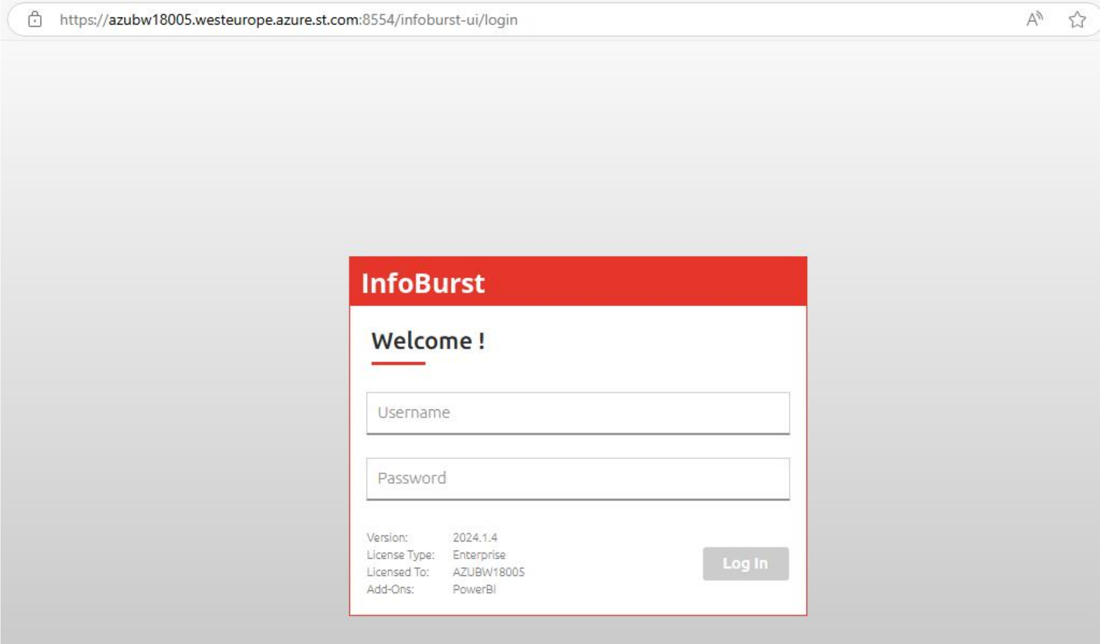
- Select **Install**

The user interface requires an HTML5-compliant web browser (Microsoft Edge/Google Chrome) and will not be rendered properly if launched in Internet Explorer.

Post-Installation

User Log In

- Browse to *http://<SERVER>:8554*
- Enter default credentials (Username: admin, Password: admin)



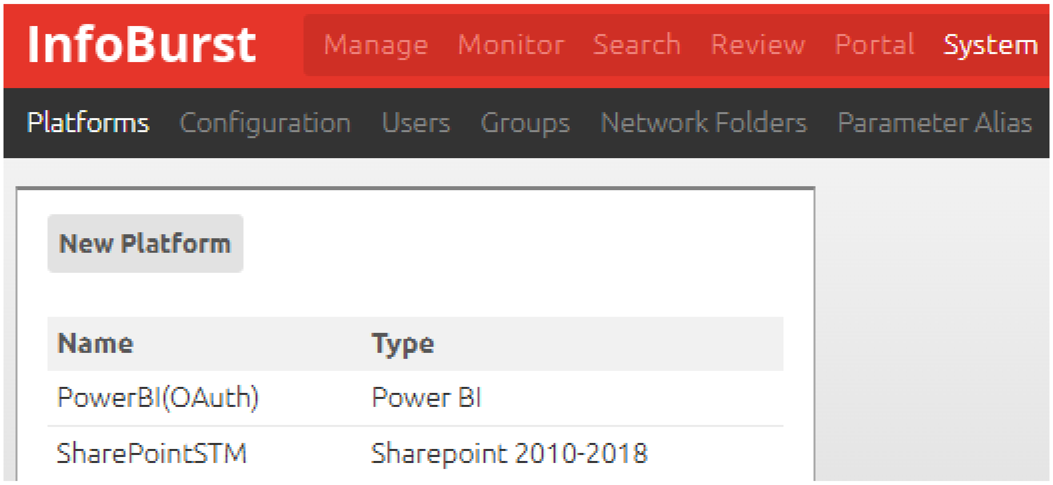
https://azubw18005.westeurope.azure.st.com:8554/infoburst-ui/login

Version:	2024.1.4
License Type:	Enterprise
Licensed To:	AZUBW18005
Add-Ons:	PowerBI

Go to the **System** option on the red bar and click on the **Platform** option in the black bar below.

Click on New Platform and make two platforms for **Power BI access** and **SharePoint 2010-2018** respectively.

Their authentication methods are discussed in detail in the next two sections.



Name	Type
PowerBI(OAuth)	Power BI
SharePointSTM	Sharepoint 2010-2018

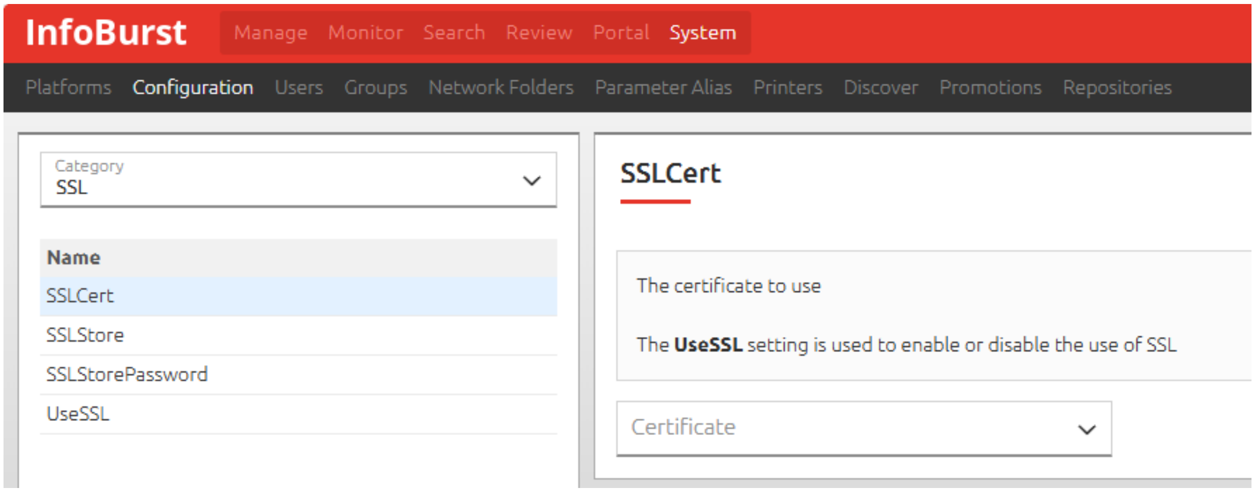
Power BI Access (OAuth)

Prerequisite

This authentication method requires a server callback from Microsoft. This callback requires InfoBurst to be SSL-enabled. See the following SSL setup instructions:

Enable SSL

- Select **System > Configuration > SSL**
- Select **SSLCert** then select the certificate



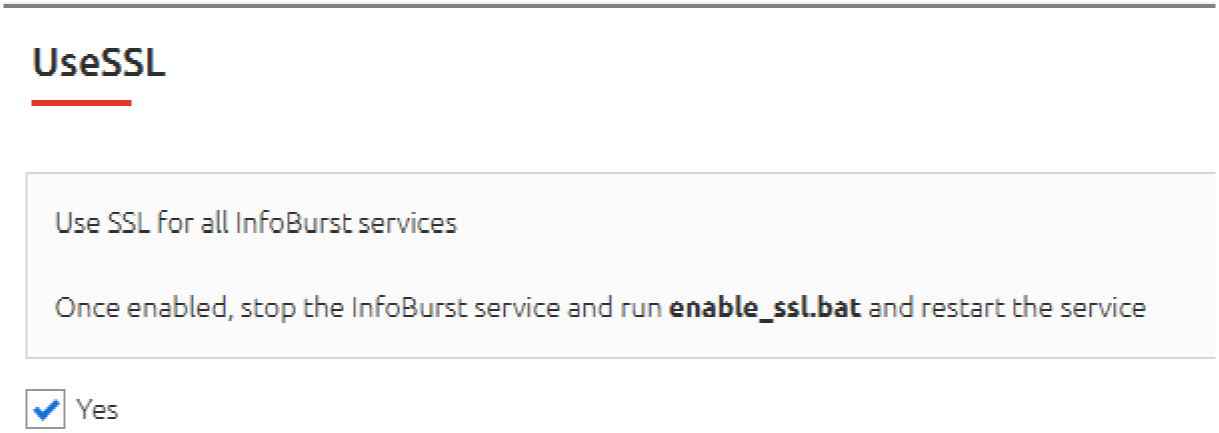
Category
SSL

SSLCert

The certificate to use

The **UseSSL** setting is used to enable or disable the use of SSL

- Select the **Save** button
- Select **UseSSL**
- Check **Yes** and select the **Save** button



UseSSL

Use SSL for all InfoBurst services

Once enabled, stop the InfoBurst service and run **enable_ssl.bat** and restart the service

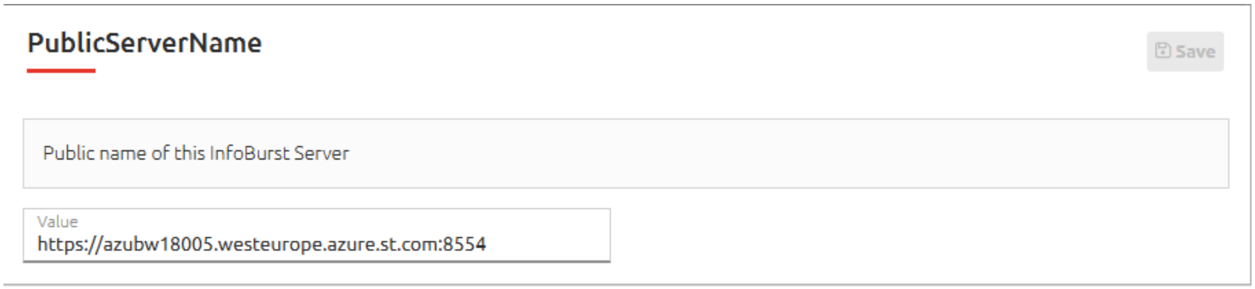
☑ Yes

- Stop the **InfoBurst** service
- Open a command prompt (Run As Administrator) and change directory to the InfoBurst application root (default = C:\Program Files\InfoSol\InfoBurst)
- Enter **enable_ssl**
- Start the **InfoBurst** service

SSL is now enabled. The InfoBurst user interface URL will now require HTTPS. Any dashboards or applications that communicate with InfoBurst via REST (default = 8551) must be updated to use HTTPS and certificate alias (Friendly Name).

Validate PublicServerName

Open **System > Configuration > PublicServerName.** The value should contain a URL that matches the certificate alias. If the value does not match, then update the value to match (example: https://acme.infoburst.com:8554) and **Save.**


PublicServerName

Public name of this InfoBurst Server

Value
https://azubw18005.westeurope.azure.st.com:8554

Change SSL Certificate

- Execute the **Disable SSL** process described above
- Install the new SSL certificate
- Execute the **Enable SSL** process described above

Step 1 (InfoBurst): Obtain Callback URI	• Select **System > Configuration > Authentication** • Select **OAuthCallbackURI** • Note value for use in Microsoft Entra ID
Step 2 (Microsoft Entra ID): Register App	• Select **App Registrations** • Select **New registration** • Enter a **Name** • Under **Redirect URI** select **Web** • Enter Callback URI from **Step 1** • Select **Register**

	• Note **Application (client) ID** and **Directory (tenant) ID** for use in InfoBurst • Select **Certificates & secrets** • Select **New client secret** • Enter **Description** • Select **Expiry** • Select **Add** • Note **Value** for use in InfoBurst
Step 3 (Microsoft Entra ID): Grant API Permissions	• Open **App registrations** • Select the App created in **Step 1** • Select **API Permissions** • Select **Add a permission** • Select **Power BI Service** • Select **Delegated permissions** • Select the following permissions: • **Dataflow > Dataflow.ReadWrite.All** • **Dataset > Dataset.ReadWrite.All** • **Report > Report.ReadWrite.All** • **Workspace > Workspace.ReadWrite.All** • Select **Add Permissions**
Step 4 (InfoBurst): Create Power BI Platform	• Select **System > Platforms > New Platform** • Select **Type > Power BI**

	- Enter **Name** - Under **Microsoft Entra ID Authentication > OAuth** enter **Application ID, Application Client Secret**, and **Directory (Tenant) ID** - Select **Save** - Select **Begin Authentication** (new Microsoft authentication tab opens). This step adds Platform Credentials only for the InfoBurst administrator user. See **User Access** below for user Platform Credentials process. - Select **Accept** - Return to InfoBurst - Select **Close**

User Access

Each InfoBurst intending to use the Power BI Platform must first add Platform Credentials: **Platform Credentials -> + -> Power BI Platform -> Begin Authentication -> Accept**

Token Maintenance

User authentication tokens issued by Microsoft can expire. Use the following process to renew an authentication token: **Platform Credentials -> + -> Power BI Platform** -> **Update Authentication -> Accept**

App Secret Expiry

The App Secret has an expiry date designated by the Microsoft Entra ID administrator. An expired Secret **will prevent** InfoBurst from authenticating to Power BI. Plan to update the Secret in Microsoft Entra ID and Power BI Platform accordingly.

SharePoint Access

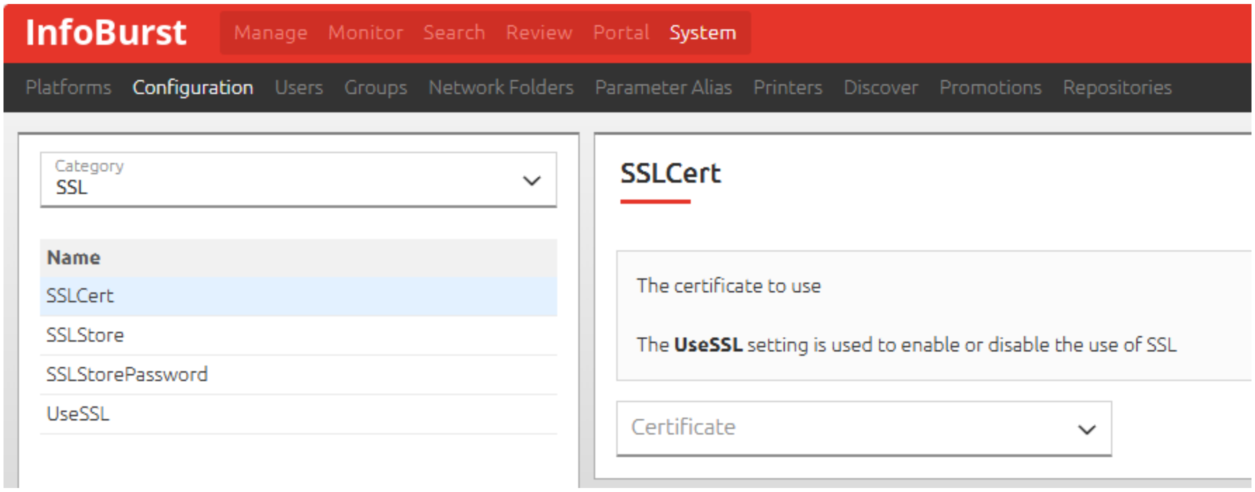
Microsoft Entra ID OAuth

Prerequisite

See the following SSL setup instructions:

Enable SSL

- Select **System > Configuration > SSL**
- Select **SSLCert** then select the certificate



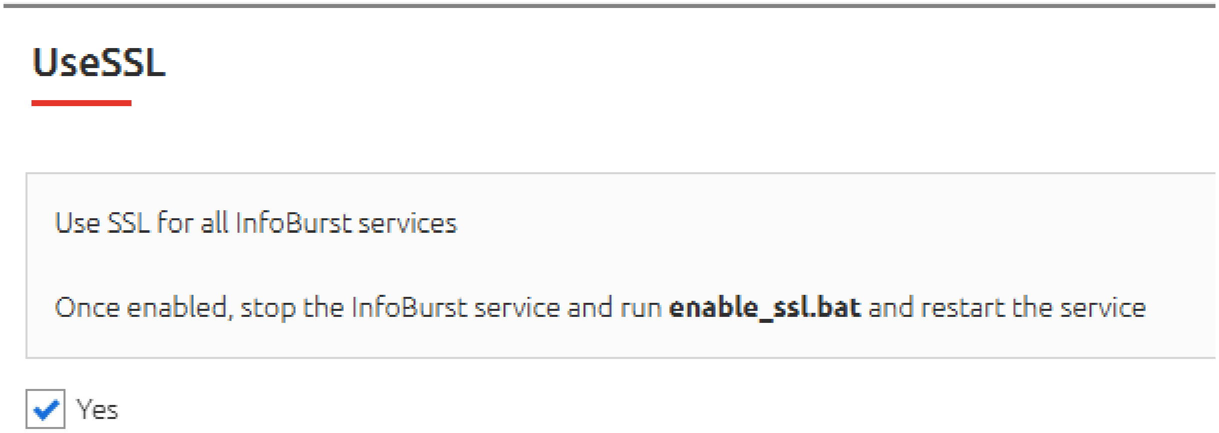
Category
SSL

SSLCert

The certificate to use

The **UseSSL** setting is used to enable or disable the use of SSL

- Select the **Save** button
- Select **UseSSL**



UseSSL

Use SSL for all InfoBurst services

Once enabled, stop the InfoBurst service and run **enable_ssl.bat** and restart the service

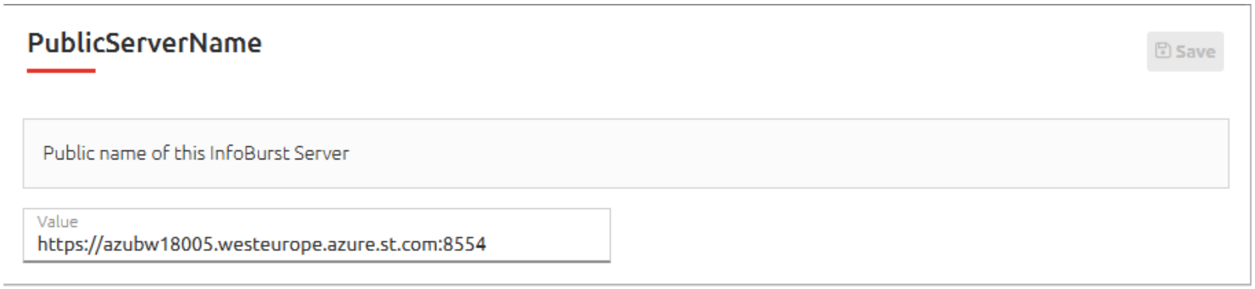
☑ Yes

- Check **Yes** and select the **Save** button
- Stop the **InfoBurst** service
- Open a command prompt (Run As Administrator) and change directory to the InfoBurst application root (default = C:\Program Files\InfoSol\InfoBurst)
- Enter **enable_ssl**
- Start the **InfoBurst** service

SSL is now enabled. The InfoBurst user interface URL will now require HTTPS. Any dashboards or applications that communicate with InfoBurst via REST (default = 8551) must be updated to use HTTPS and certificate alias (Friendly Name).

Validate PublicServerName

Open **System > Configuration > PublicServerName**. The value should contain a URL that matches the certificate alias. If the value does not match, then update the value to match (example: https://acme.infoburst.com:8554) and **Save**.


PublicServerName

Public name of this InfoBurst Server

Value
https://azubw18005.westeurope.azure.st.com:8554

Change SSL Certificate

- Execute the **Disable SSL** process described above
- Install the new SSL certificate
- Execute the **Enable SSL** process described above

Step 1 (InfoBurst): Obtain Callback URI	• Select **System > Configuration > Authentication** • Select **OAuthCallbackURI** • Note value for use in Microsoft Entra ID
Step 2 (Microsoft Entra ID): Register App	• Select **App Registrations** • Select **New registration** • Enter a **Name** • Under **Redirect URI** select **Web** • Enter Callback URI from **Step 1** • Select **Register** • Note **Application (client) ID** for use in InfoBurst • Select **Certificates & secrets**

	• Select **New client secret** • Enter **Description** • Select **Expiry** • Select **Add** • Note **Value** for use in InfoBurst
Step 3 (Microsoft Entra ID): Grant API Permissions	• Open **App registrations** • Select the App created in **Step 1** • Select **API Permissions** • Select **Add a permission** • Select **SharePoint** • Select **Delegated permissions** • Select **AllSites.Manage** • Select **Add Permissions**
Step 4 (InfoBurst): Create SharePoint Platform	• Select **System > Platforms > New Platform** • Select **Type > SharePoint** • Enter **Name** • Enter **SharePoint Site URL** (example: https://acme.sharepoint.com/Accounting) • Select **Authentication > Microsoft Entra ID OAuth** • Enter **Application ID** and **Application Client Secret** • Select **Save** • Select **Begin Authentication** (new Microsoft authentication tab opens). This step adds Platform

	Credentials only for the InfoBurst administrator user. See **User Access** below for user Platform Credentials process. • Select **Accept** • Return to InfoBurst • Select **Close**

User Access

Each InfoBurst intending to use the SharePoint Platform must first add Platform Credentials: **Platform Credentials -> + -> SharePoint 2010-2018** -> **Begin Authentication -> Accept**

Token Maintenance

User authentication tokens issued by Microsoft can expire. Use the following process to renew an authentication token: **Platform Credentials -> + -> SharePoint 2010-2018** -> **Begin Authentication -> Accept**

App Secret Expiry

The App Secret has an expiry date designated by the Microsoft Entra ID administrator. An expired Secret **will prevent** InfoBurst from authenticating to SharePoint. Plan to update the Secret in Microsoft Entra ID and SharePoint Platform accordingly.