One-Way SSL Implementation in BOOMI

Author

Shamik Roy Chaudhury

In this blog, we will cover how we can implement One-way SSL in Boomi.

What is SSL?

SSL stands for Secure Sockets Layer. It's a protocol designed to provide secure communication over a computer network, typically the Internet. SSL ensures that the data exchanged between a web server and a client (such as a web browser) remains encrypted and thus protected from eavesdropping, tampering, and forgery.

Here's how SSL works:

- **Handshake**: The SSL handshake is the initial step in establishing a secure connection. During this process, the client and the server agree on encryption methods and exchange cryptographic keys.
- **Encryption**: Once the handshake is complete, SSL encrypts all data transferred between the client and the server using symmetric encryption. This means that even if intercepted, the data is indecipherable without the appropriate decryption key.
- **Data Integrity**: SSL also ensures data integrity, meaning that the data cannot be altered or tampered with during transmission. It achieves this through the use of cryptographic hashes and message authentication codes (MACs) that detect any unauthorized changes to the data.

Authentication: SSL can also provide authentication, allowing the client to verify the identity of the server (and optionally vice versa). This helps prevent man-in-the-middle attacks where a malicious third party impersonates the server to intercept or alter the communication.

SSL has evolved over time, and its successor, Transport Layer Security (TLS), is now more commonly used. However, the term "SSL" is still often used colloquially to refer to both SSL and TLS protocols.

SSL/TLS is widely used to secure various types of online communication, including web browsing, email, instant messaging, and file transfers. Websites that use SSL/TLS have URLs starting with "https://" instead of "http://", indicating a secure connection.

- One-way SSL (Secure Sockets Layer) and Two-way SSL (also known as mutual SSL) are configurations of SSL/TLS that differ in the way authentication is performed between the client and the server.

©TGH Software Solutions Pvt. Ltd.

One-way SSL:

- In one-way SSL, only the server is required to present a digital certificate to the client to establish a secure connection.
- The client verifies the server's certificate to ensure it is trusted and authenticates the server's identity.
- The server's certificate typically contains information such as the server's public key, its validity period, and information about the certificate authority that issued it.
- Once the server's identity is verified, the client and server establish an encrypted connection using symmetric encryption.

Now, let's see the steps to implement One-way SSL in Boomi.

Step 1: First, log on to the **Boomi platform** (https://platform.boomi.com/) with a **username** and **password**.
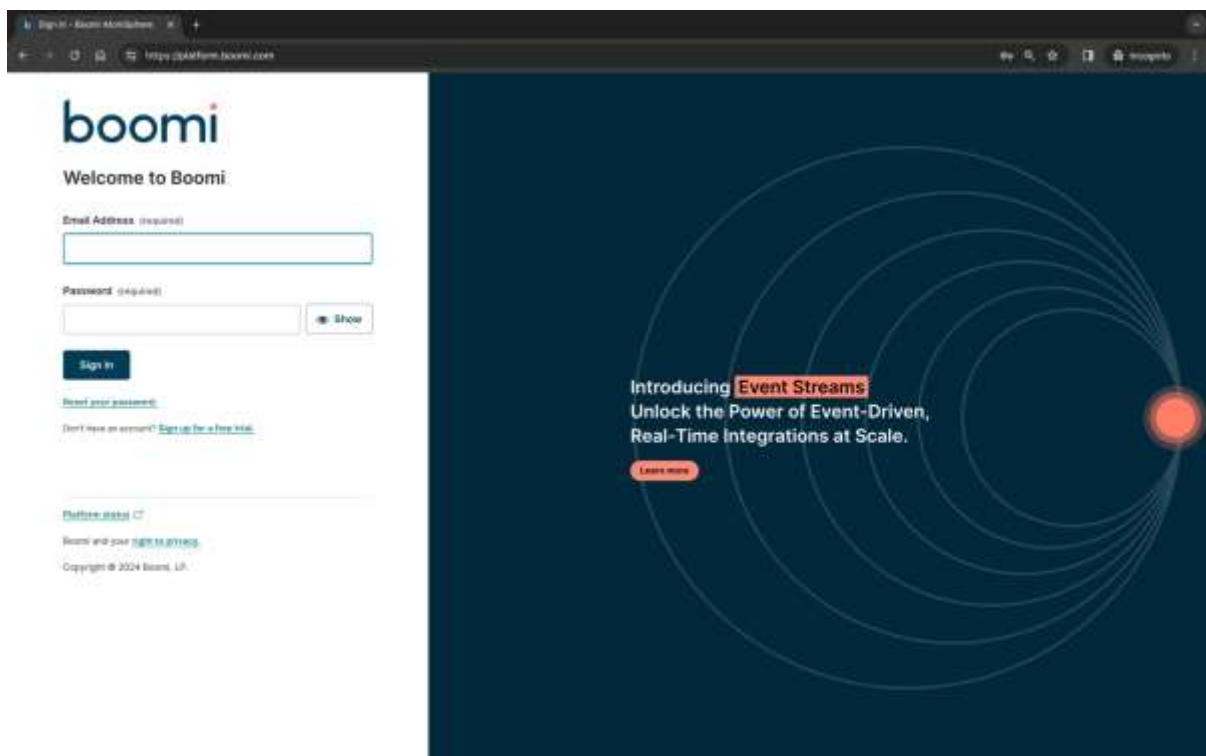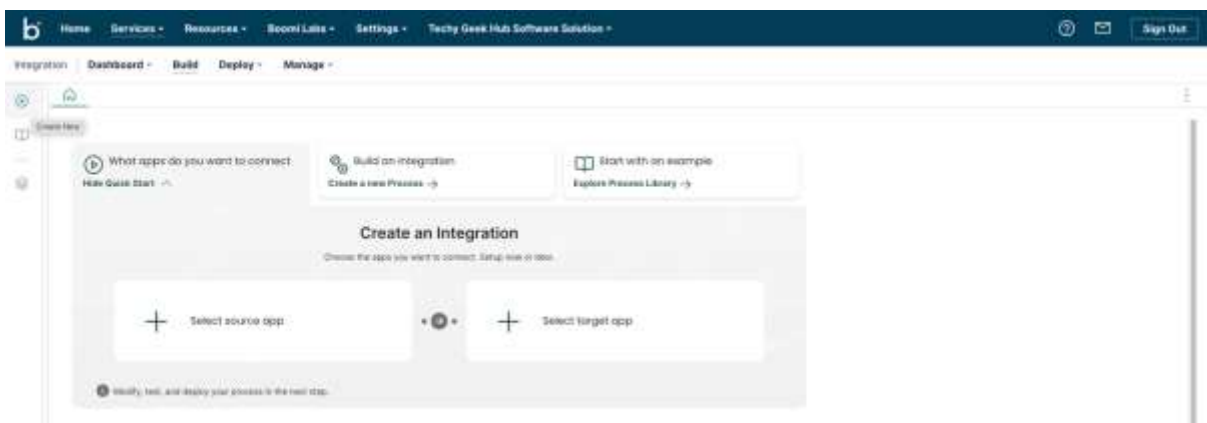
Step 2: Once, you have logged into the Boomi platform, you can view the **Home** page.
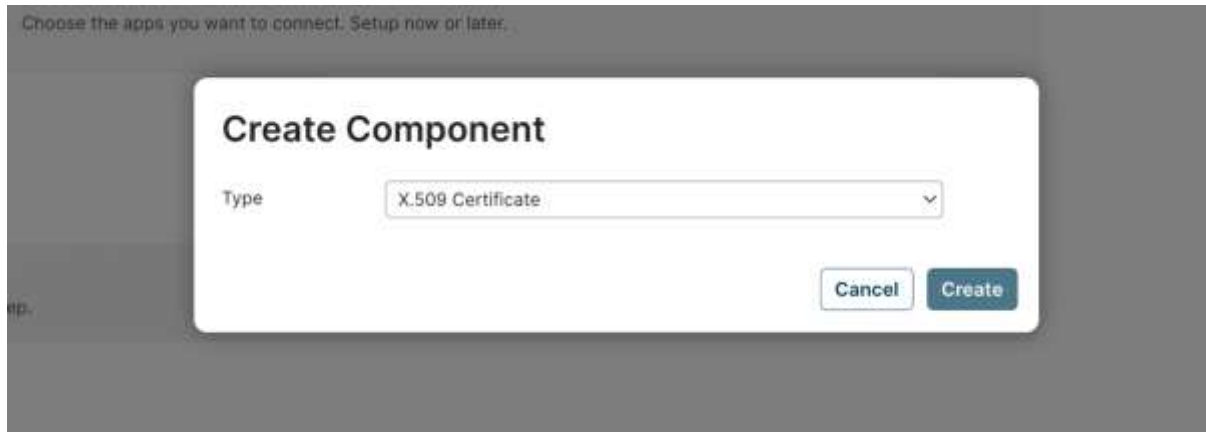

Step 3: Now, click on **Services** followed by **Integration**. You will see the Build page.
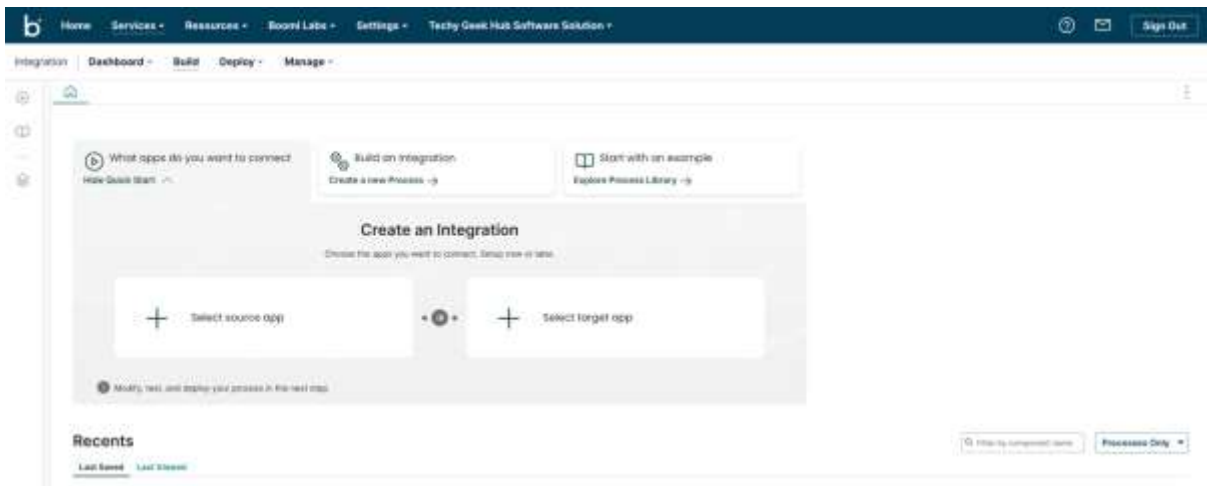
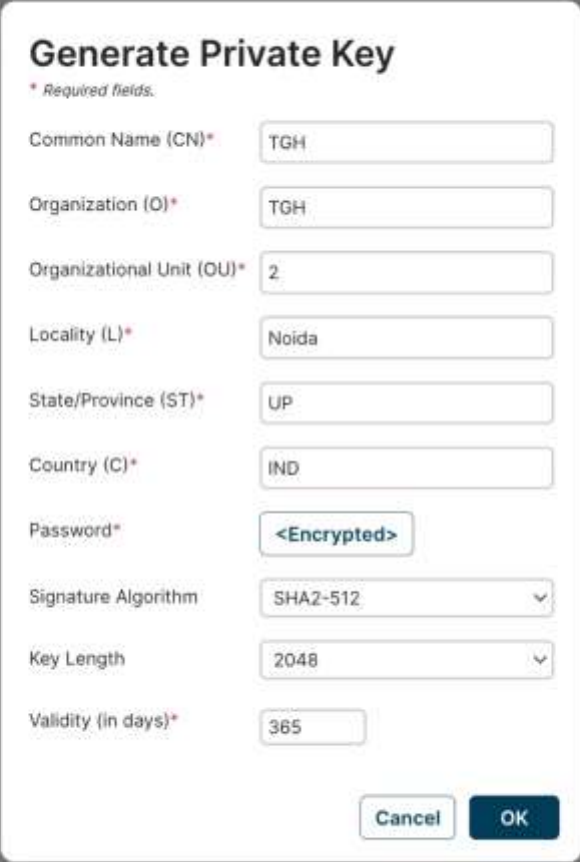**Step 4:** Now click on **Create new**.

Step 5: Choose the Component type as **X.509 certificate**, then click on **Create.**

Step 6: Give a name for the certificate and click on **Generate.**

Step 7: Fill in all the details related to the certificate. Click on **OK**.

Step 8: Now the certificate will be generated. Click on save and then **Export Public Cert** and **Export Private Key.**

Step 9: Now create two certificates. (*Follow Steps 4-5*) One for the Public key and another for the Private key. Then on one certificate Click on **import** and choose the public key (*from your device where you have downloaded the certificates in step 8*) to generate the public certificate and on another certificate Click on **import** and choose the private key (*from your device where you have downloaded the certificates in step 8*) to generate the private certificate.

- Please select a file containing a private key (.pfx, .p12) or public cert (.cer, .der).
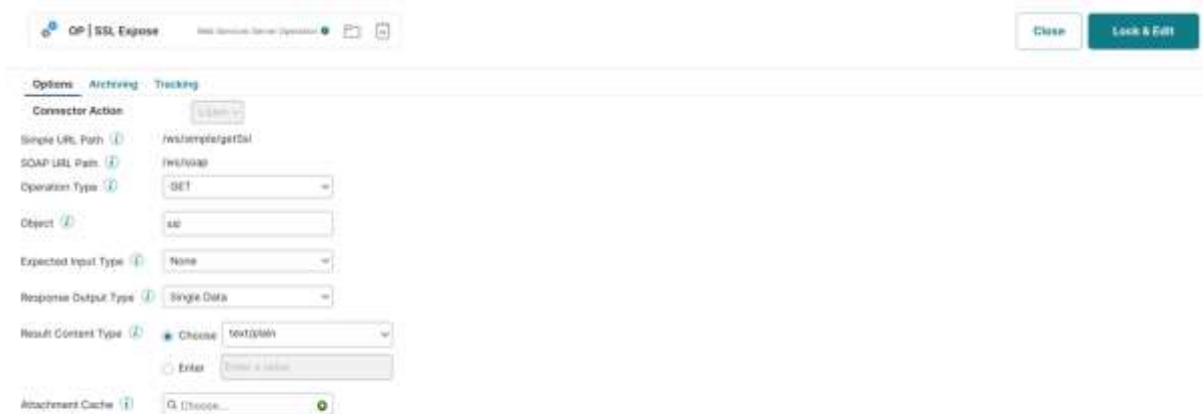

©TGH Software Solutions Pvt. Ltd.

- In the case of importing private certificates, we have to provide the password. (*same password set at step 7*)

Step 10: Now we have exposed one API from Boomi Atomsphere**.** For that **create a new process.** Choose **Start shape** with **Web Services Server.** Set **Action** as **Listen.** Create One **Operation.**
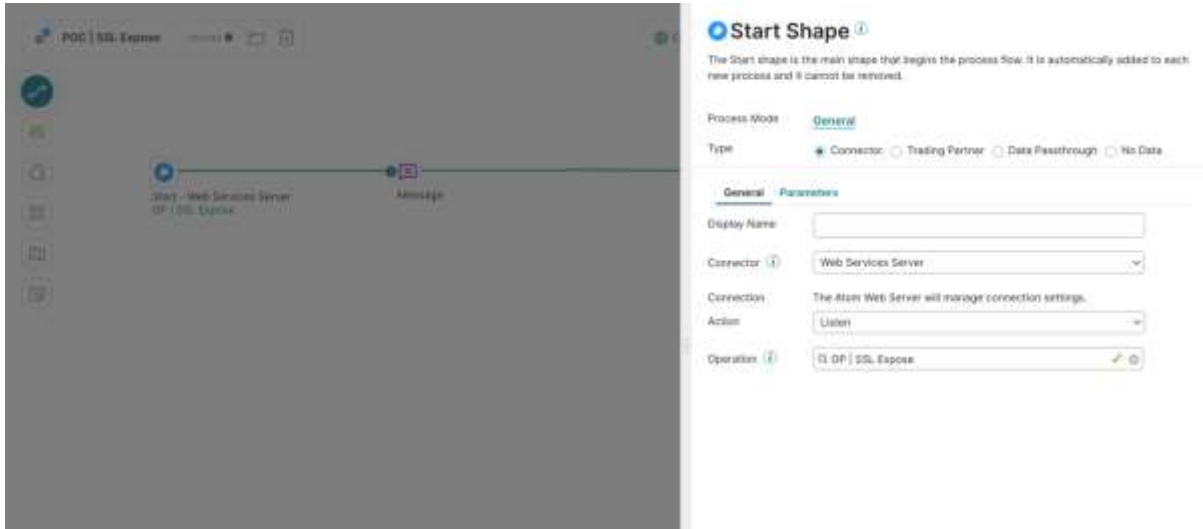
Step 11: Configure the **Operation.** Set the **Operation type,** give the Object name on **Object,** select the **request** and **response type** and click on **'Save & Close'.**
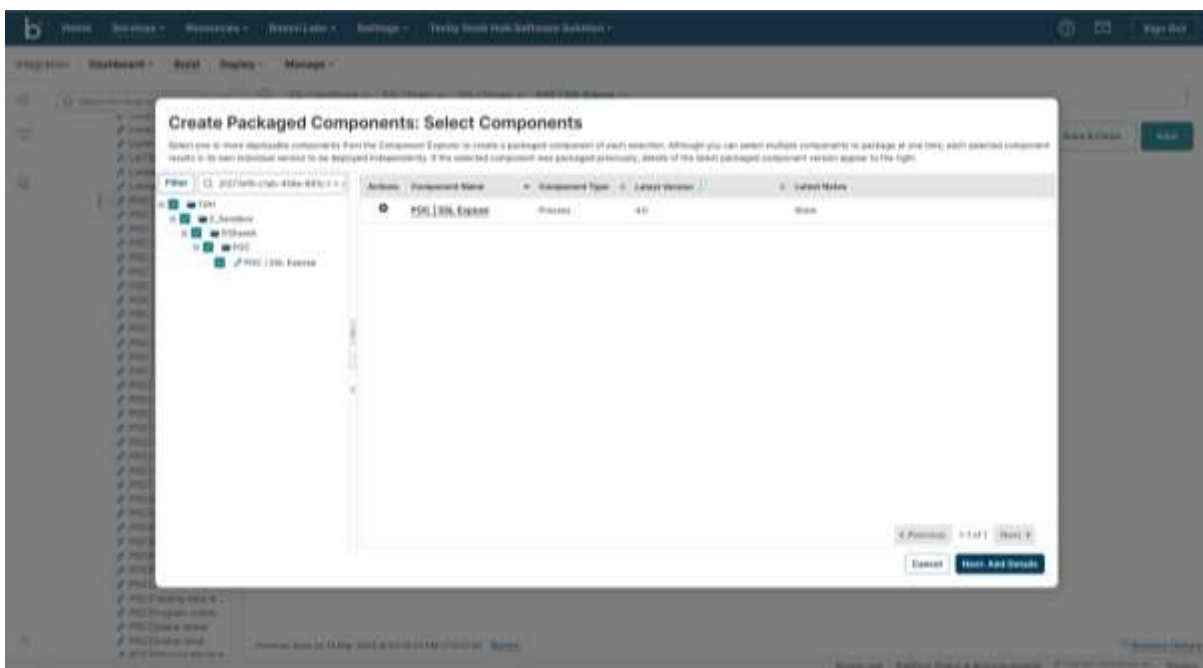
Step 12: Take a **message** shape and set the text **'Hi, Shamik Roy Chaudhury'**.
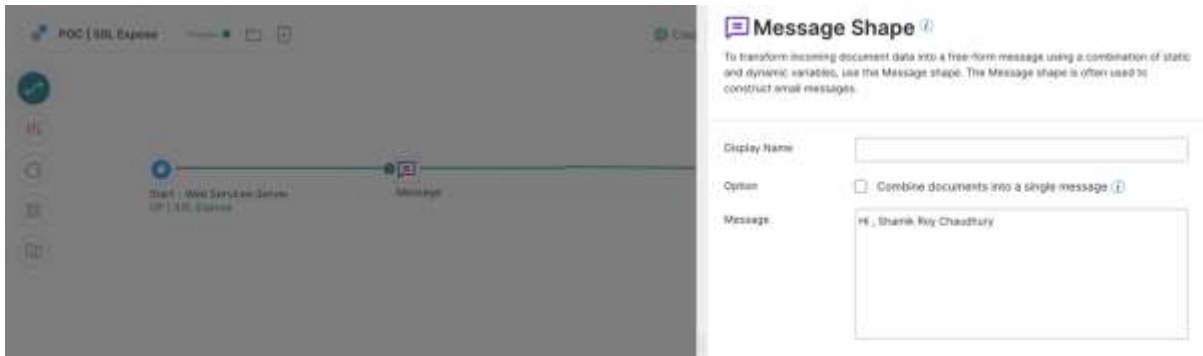
Step 13: Now place a **Return Document** shape. Then click on **Create Packaged Component**.

Step 14: Click on **Add details.**
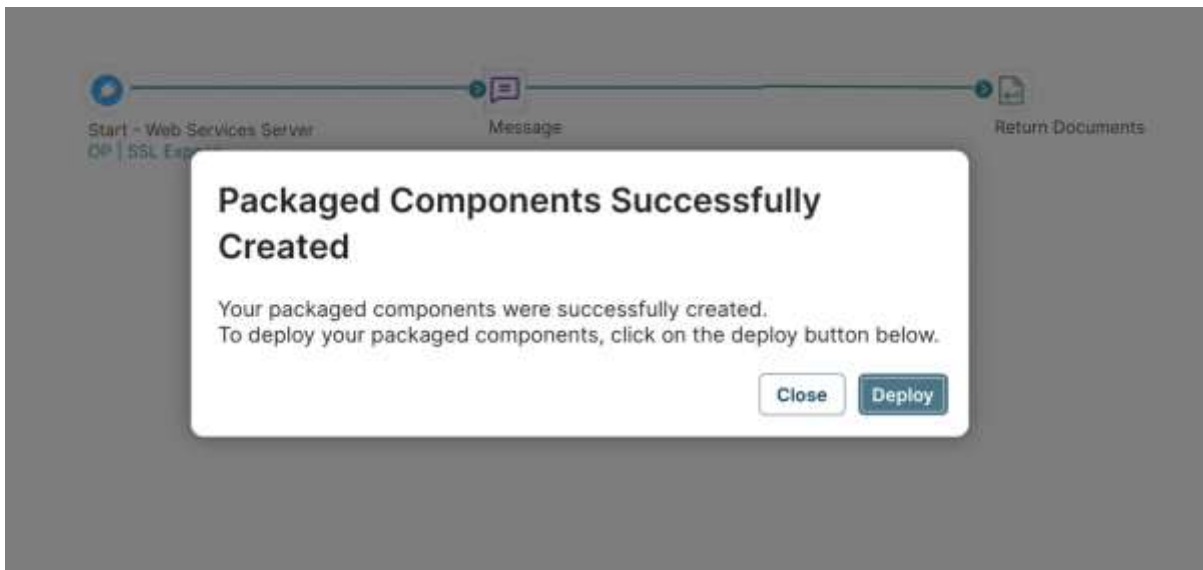

©TGH Software Solutions Pvt. Ltd.

Step 15: Click on the **Create Packaged Component.**

Step 16: Click on **Deploy.**

Step 17: Choose the **Environment** and click on **Next: Select Versions**.
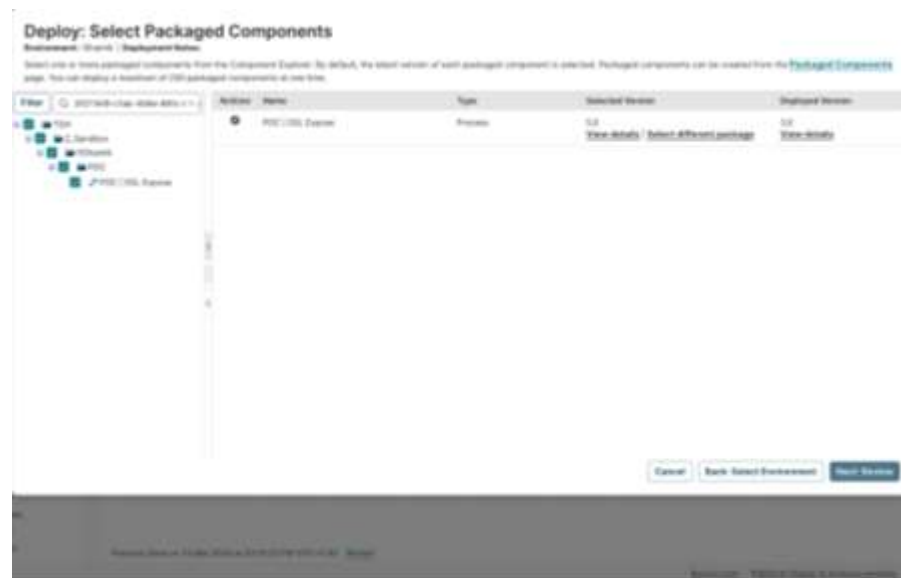
Deploy: Select Environment

Select the environment in which to deploy your packaged component(s), and optionally add notes about the deployment.

Deployment Environment   Q 1Shamik

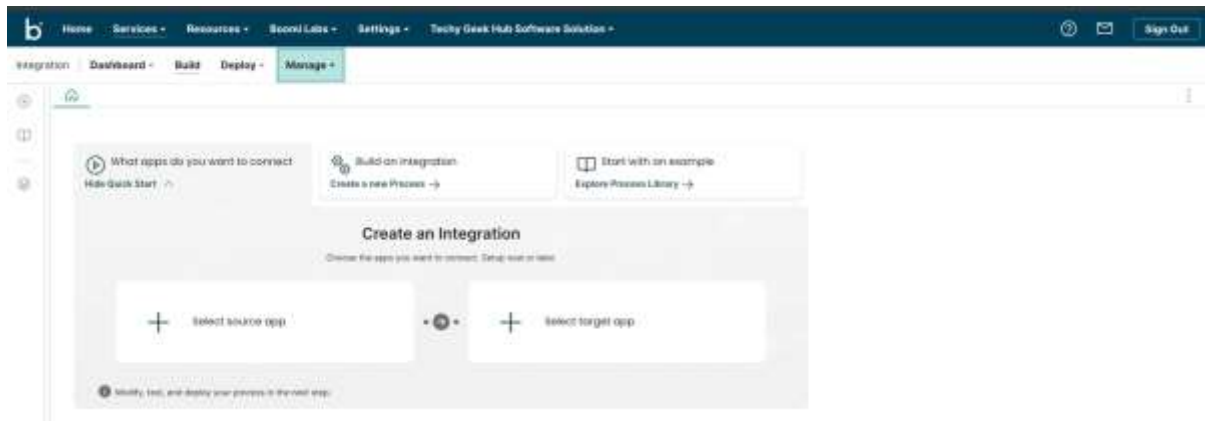Deployment Notes   [   ]

-4000 characters remaining.

[Cancel] [Next: Select Versions]

Step 18: Click on **Next: Review**.

Deploy: Select Packaged Components

Select one or more packaged components from the Component Explorer. By default, the latest version of each packaged component is selected. Packaged components can be created from the **Packaged Components** page. You can deploy a maximum of 200 packaged components at one time.

Actions	Name	Type	Selected Version	Deployed Version
○	PRC SSL Expose	Process	5.0 View details / Select different package	5.0 View details

[Cancel] [Back: Select Environment] [Next: Review]

Step 19: Click on **Deploy.**

Step 20: Click on **Manage**.

Step 21: Now click on **Atom Management**.

Step 22: Go to your **Atom > Shared web server.** Set the **API type** as **Basic.** In **Listening Port Configuration,** check the **SSL** checkbox. And in the **SSL Certificate** add the Private certificate.
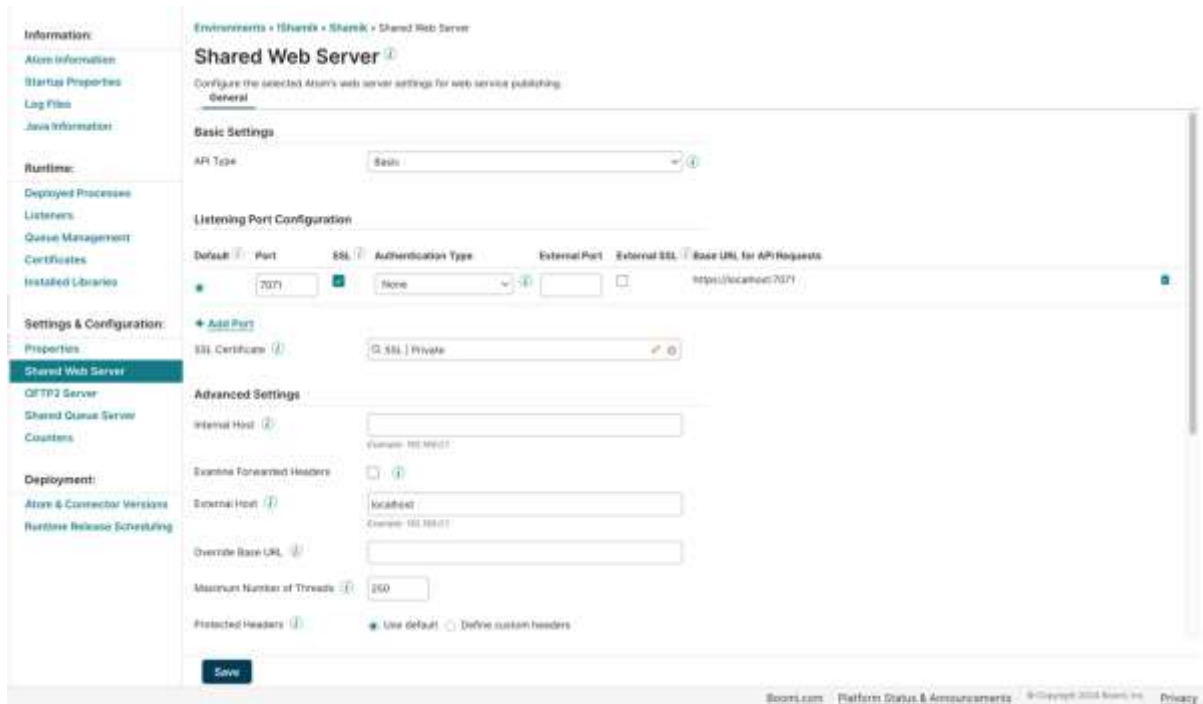

Step 23: Create a new process for consuming the API that we just exposed. Create a process which starts with **Start** shape with **No Data** type. Then take an **HTTP client connector**.

Step 24: Configure the connection of the HTTP client connector. Create a connection, and provide the URL (Base URL from shared web server + simple path from shared web server operation).
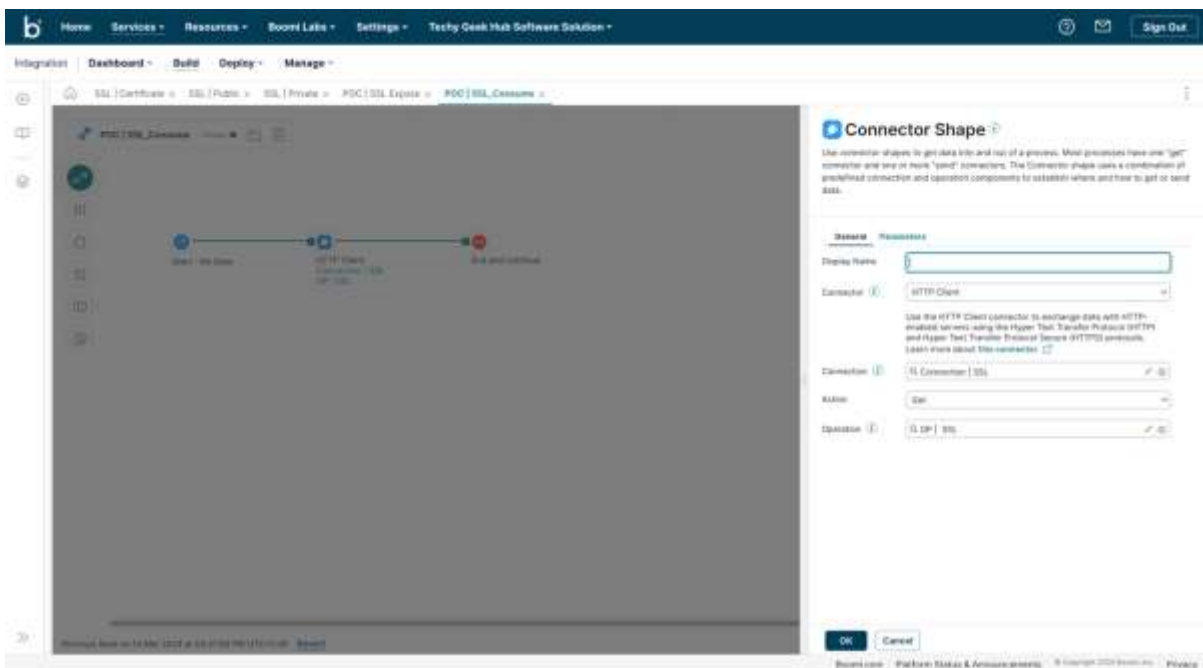

©TGH Software Solutions Pvt. Ltd.

Step 25: Go to **SSL options** in the connection, Check the checkbox **Use Trusted SSL Certificate** and below add the Public certificate in the **Trust SSL Server Certificate**.
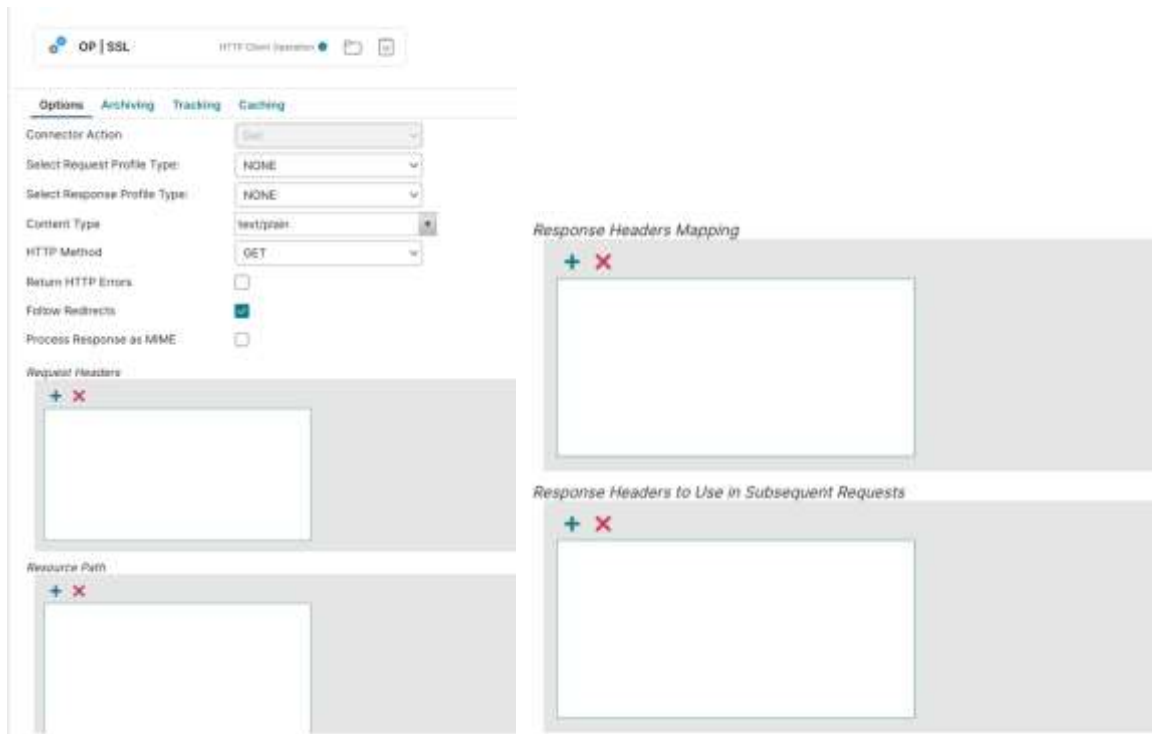
Click on **Save & Close**.
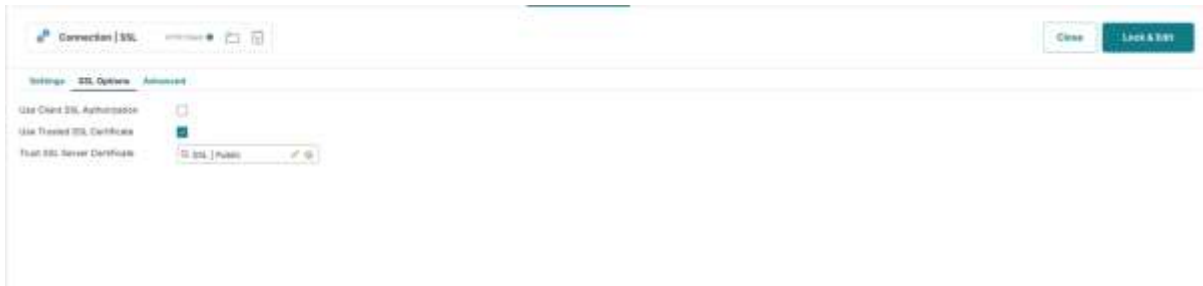
Step 26: Set the Action as **Get**. Create an operation.

Step 27: Configure the operation. Then click on **Save & Close**.
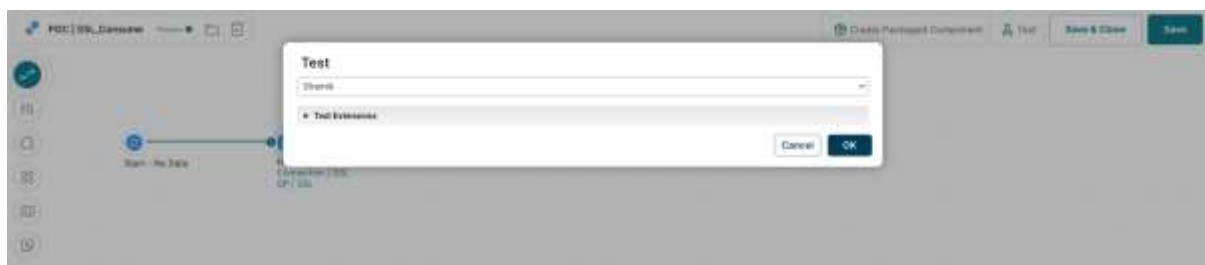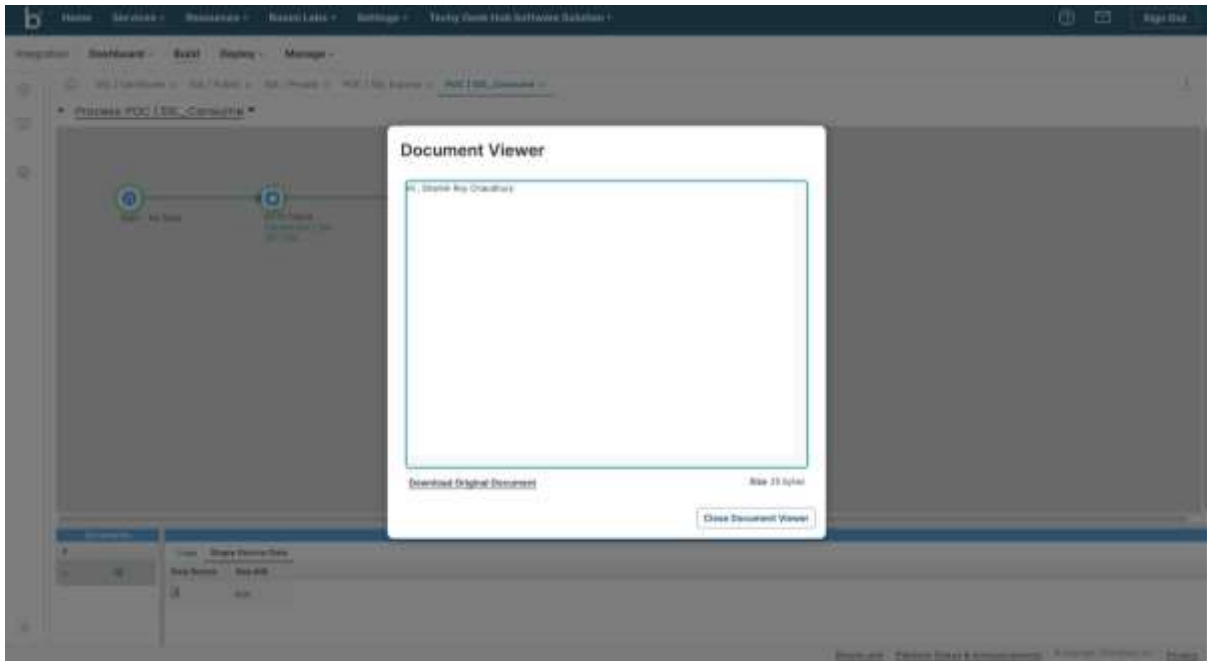
©TGH Software Solutions Pvt. Ltd.

Step 28: Put a **stop** shape. And Hit the **test** button.

Step 29: Choose the **runtime engine** and Click on **OK**.

Step 30: Click on **Stop** Shape. Click on **Shape Source Data.**

TGH

Making Integrations Simpler

TGH Software Solutions Pvt. Ltd.

www.techygeekhub.com

At TGH, we specialize in driving digital transformation through seamless Integration Technologies.

Operating as an INTEGRATION FACTORY, we serve as a one-stop shop for all your integration needs. Our expert team is well-versed in enterprise software and legacy system integration, along with leading iPaaS technologies like Boomi, MuleSoft, Workato, OIC, and more.

We're committed to enhancing business processes and solving problems through our integration expertise.

Email address
connect@techygeekhub.com

Phone number
+ 011-40071137
+ 91-8810610395

Our offices

Noida Office
iThum
Plot No -40, Tower A,
Office No: 712,
Sector-62, Noida,
Uttar Pradesh, 201301

Hyderabad Office
Plot no: 6/3, 5th Floor,
Techno Pearl Building,
HUDA Techno Enclave,
HITEC City, Hyderabad,
Telangana 500081