

Secure Gateway

Hybrid Integration Enablement

October 2017

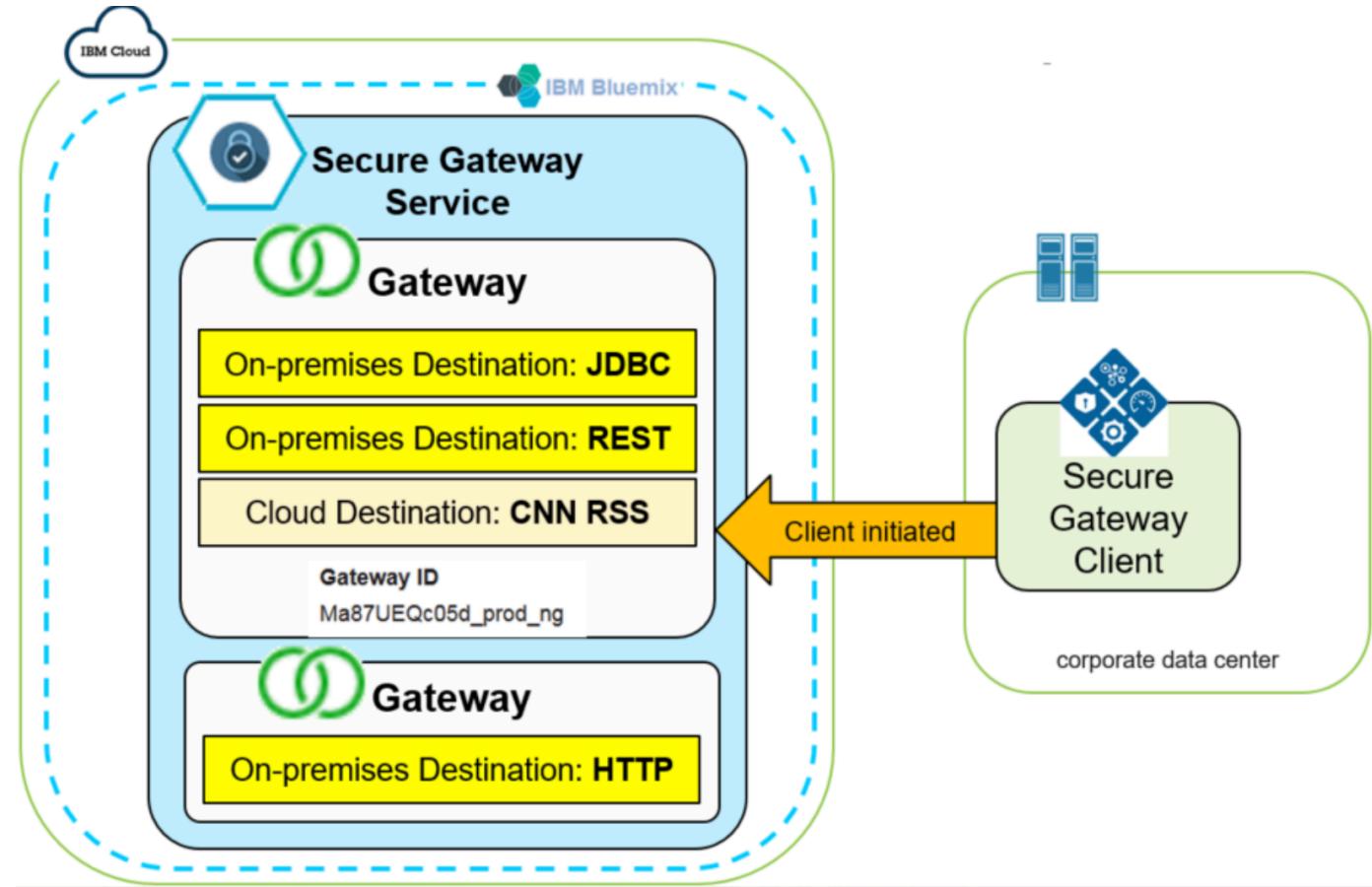


General Conversation

- The Secure Gateway provides secure connectivity and establishes a tunnel between your Bluemix organization and the remote location where you want to connect.
- Secure Gateway provides secure way to connect Bluemix applications to remote locations on-premises or in the cloud.
- https://console.ng.bluemix.net/docs/services/SecureGateway/secure_gateway.html

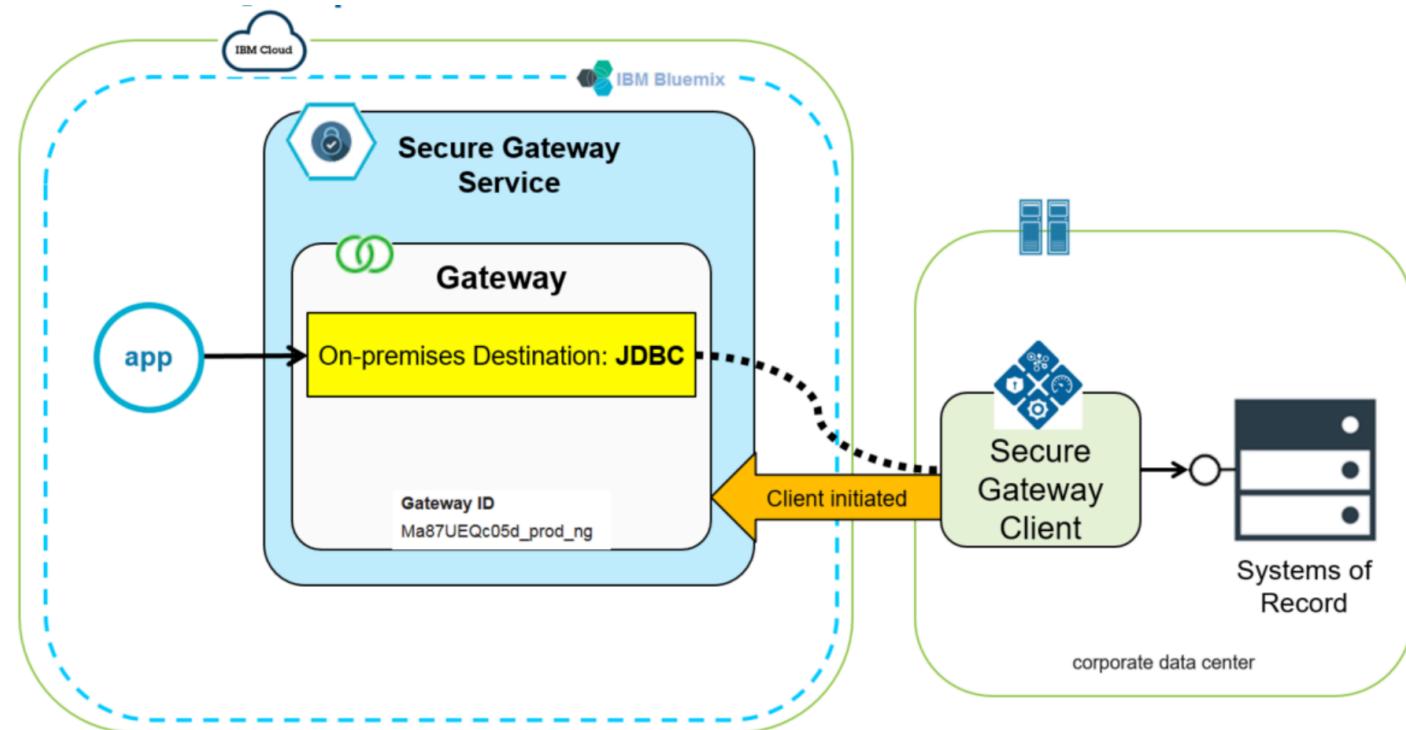
Secure Gateway Concept

- In the secure gateway configuration, the Secure Gateway service defines one or more gateways. The gateways are identified by the Gateway IDs. The Secure Gateway client initiates connection to the Gateway based on the Gateway ID. The gateway ID contains the destination information.
- The secure gateway client runs on DataPower appliances or as a Node.js program.



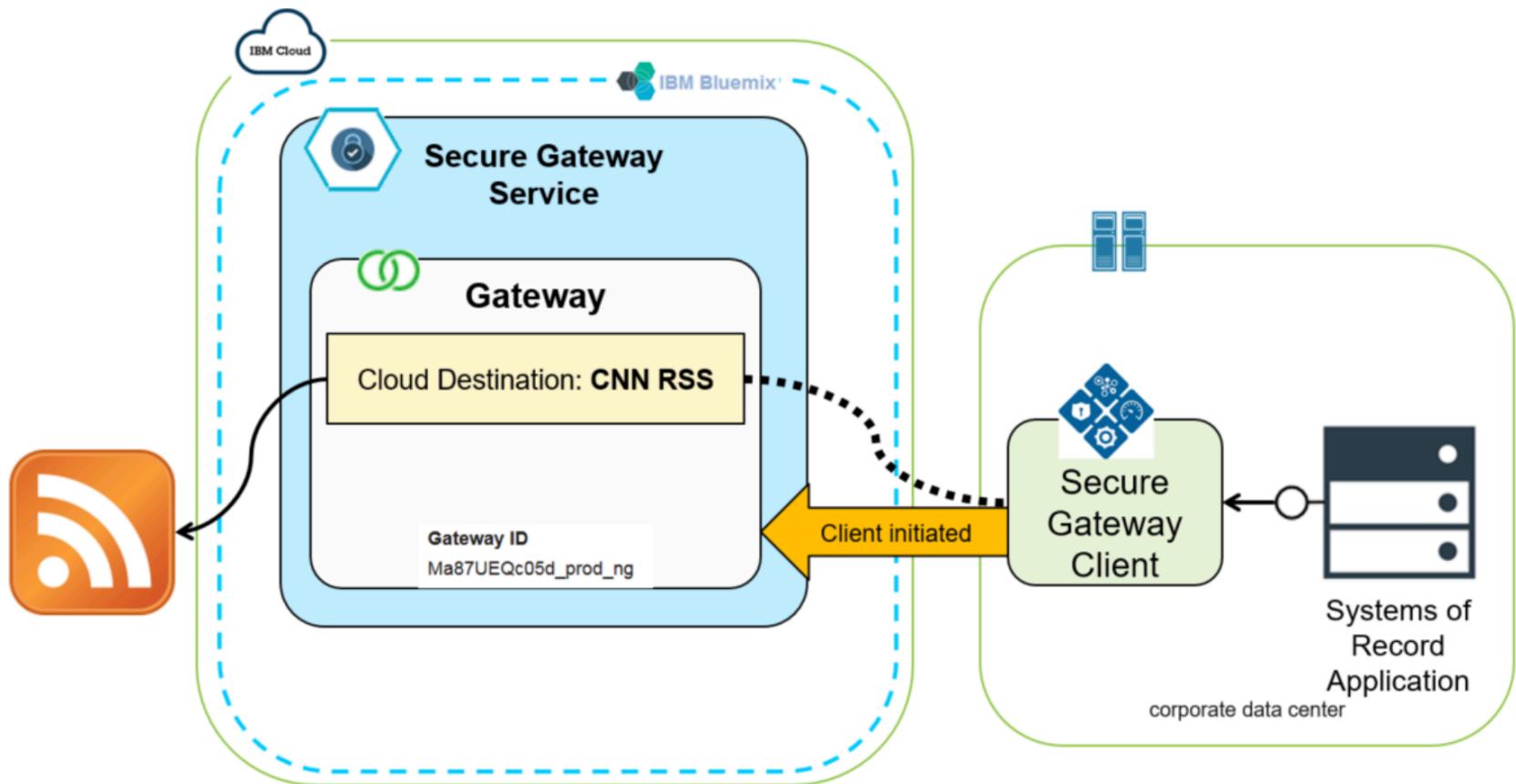
Secure Gateway on-premises destination

- For the on-premises destination to be available for a program running in the cloud, Secure Gateway open a host and port pair that is mapped to the on-premises host and port for a System of Record application.



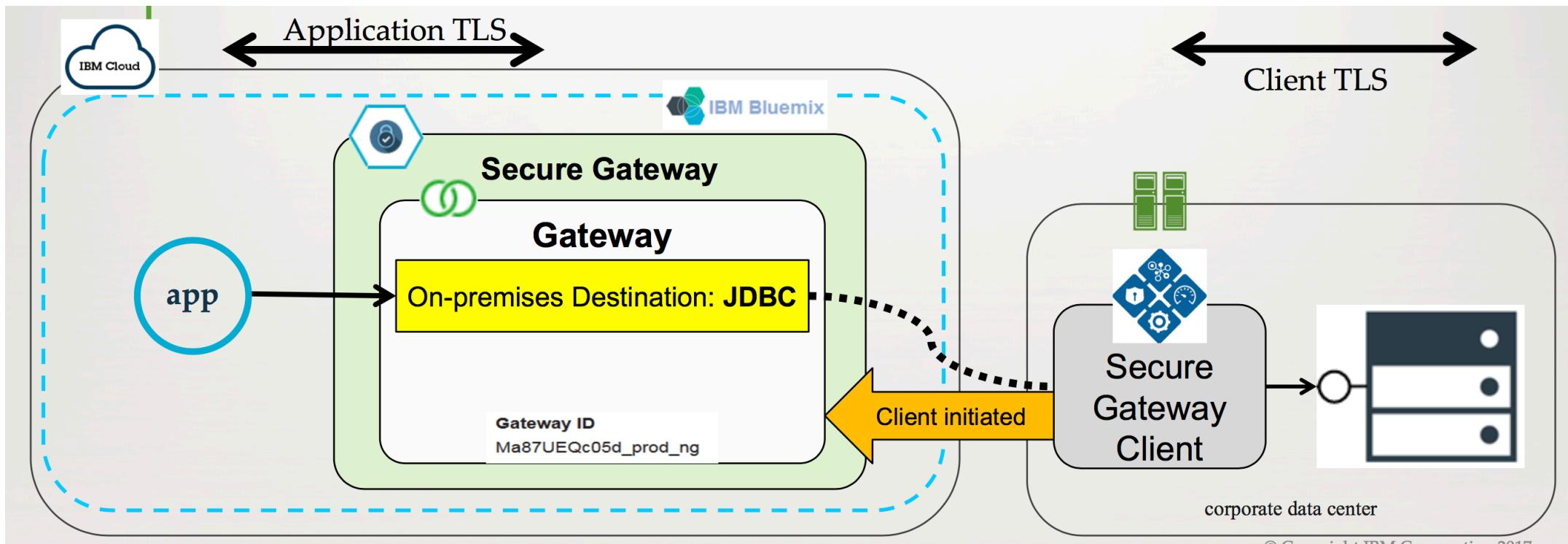
Secure Gateway cloud destination

- Secure Gateway can provide a reverse mapping for a cloud destination to be available on-premises without exposing the application directly to the internet. Secure Gateway maps a host and port from the internet to a local port on the machine that host the Secure Gateway client.



Security Overview

- Application-side TLS provides TLS between the Bluemix application to the Secure Gateway mapped gateway point.
Client-side TLS provides TLS between the client and the application.



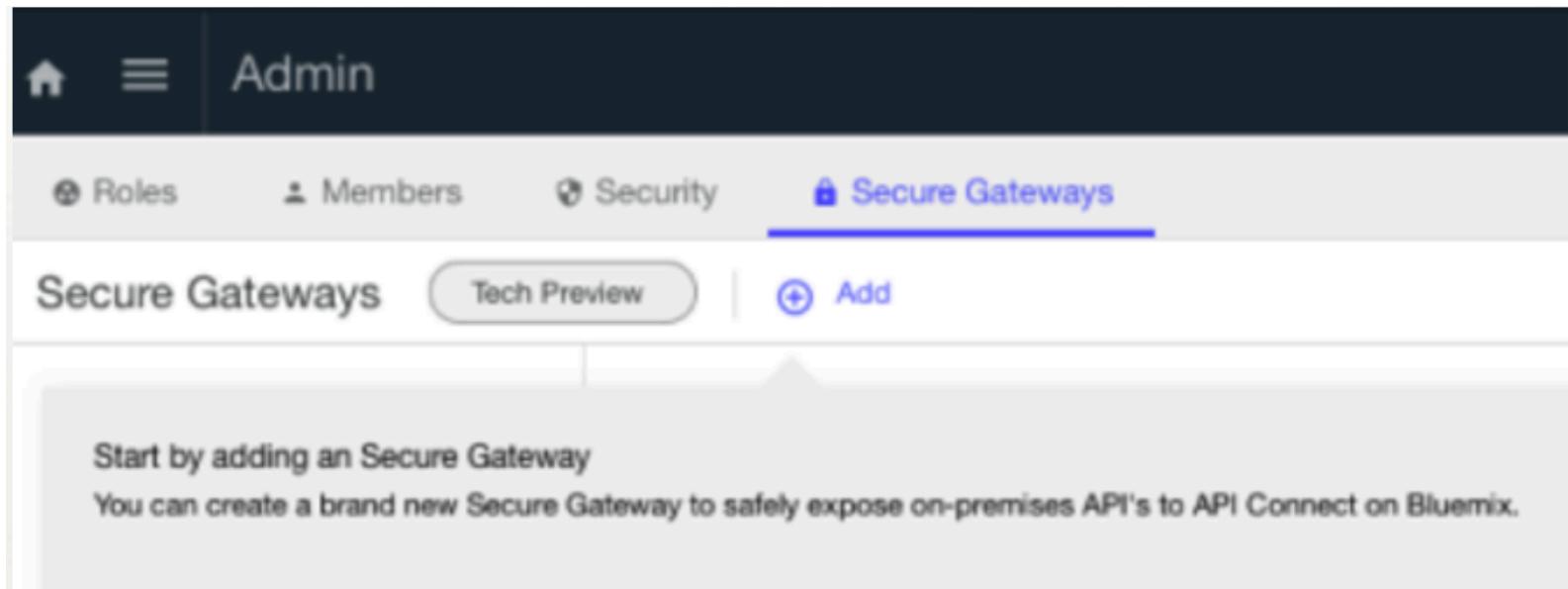
New Secure Gateway – APIC Integration

- **Built-in secure connectivity** in **Bluemix** to API backends on-premises or 3rd party clouds (Amazon, Microsoft, Google, etc) to **accelerate cloud adoption** and **reduce time to market**
- Secure connectivity to **one remote destination included for free** in every API Connect account, for both Subscription & PayGo, in **Bluemix Public**
- Additional destinations can be added via subscription for Bluemix Secure Gateway Professional OR Enterprise plans

The screenshot displays the IBM API Connect interface. At the top, there's a navigation bar with links for 'Go to Classic Experience', 'Docs', a user count of '354', and a user profile for 'Jason'. Below the navigation is a dark header with the 'Admin' tab selected. The main content area has two tabs: 'Secure Gateways' (selected) and 'Tech Preview'. Under 'Secure Gateways', there's a table with one row for a gateway named 'test'. The table columns include Name, Status, Active Clients, Destinations, ID, and Token. The 'test' row shows Enabled status, 1 active client, 0/50 destinations, ID YNEixhVbQlm_test_ng, and Token eyJhbGciOiJIUzI1Nl... . Below the table are sections for 'Secure Gateway Clients' (listing one client connected), 'Allowed Hosts and Paths', and 'Denied Hosts and Paths'. To the right of the main content is a sidebar titled 'Secure Gateways' with a numbered list of steps: 1. Create a Secure Gateway, 2. Set up a Secure Gateway client, 3. Use the Secure Gateway Client Dashboard to authorize access to your back end API's, 4. Configure the Invoke and Proxy policies of your API's to leverage the Secure Gateway, and 5. Publish your API product. At the bottom of the screenshot, there's another smaller window showing the 'Assemble' editor with a simple flow diagram.

Quickly and safely expose on-premises APIs to API Connect on Bluemix

- The Bluemix Secure Gateway Service provides secure connectivity from Bluemix to other applications and data sources running on-premises. Previously, developers would have to setup their Secure Gateway Environment and manually configure their APIs within API Connect to use it. This was often tedious and cumbersome. In this webinar, we will use Bluemix API Connect with the new Secure Gateway Integration to quickly and safely create an API for a RESTful service running on-premises



Exposing on-premises APIs through a secure gateway

- You can create a secure gateway to safely expose on-premises APIs to IBM® API Connect for Bluemix™
When you create a secure gateway, you integrate the features of the Bluemix Secure Gateway service with API Connect. This means that you have a secure way to access your on-premises APIs from API
- Connect through a secure passage without the need to provision a separate instance of the Bluemix Secure Gateway service. Effectively you create a tunnel to API Connect on a public environment without exposing your on-premises data. All that you need to do is create the gateway and attach it to an API. The creation of a destination, SSL profile, and certificates are all completed for you.

Creating a secure gateway

- When you create a secure gateway, a gateway ID and security token is generated for you.
- You also set up a secure gateway client on your on-premises environment for API Connect to connect with. After the client is set up, you use the gateway ID and security token to connect to the client so that you can access your on-premises APIs.

The screenshot shows the IBM Cloud Secure Gateways interface. At the top, there are tabs for Roles, Members, Security, and Secure Gateways, with Secure Gateways being the active tab. Below this, a list of secure gateways is shown, with one named "mysql_gateway" selected. The "mysql_gateway" row includes fields for Name (mysql_gateway), Status (ENABLED), and Active Clients (0). To the right of this row, a red box highlights the "ID" and "Token" fields. The "ID" field contains the value "z83rkDU1Nan_qabare_dec" and the "Token" field contains the value "eyJhbGciOiJIUzI1NiIsInR5c".

Set Up Secure Gateway Clients

Client Type
IBM Installers

1 Download a software installer. 2 Review the [Bluemix docs](#) or the included README.md file. 3 Install and configure client.

Software Installers

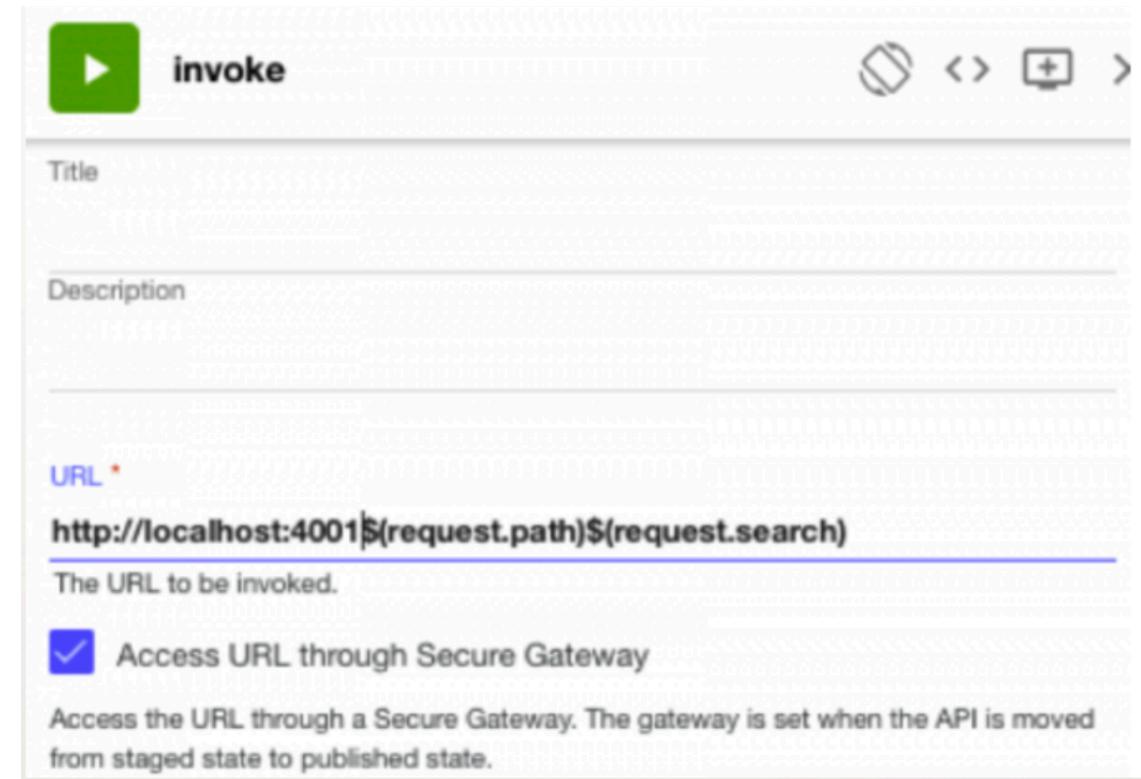
Platform	File Size
Ubuntu 14+	10.41 MB
Ubuntu 14+ PPC	9.82 MB
Ubuntu Z-Linux	10.11 MB
Windows	12.89 MB
Mac OSX	64 MB
RHEL 6+	15.56 MB

Secure Gateway Credentials

ID	z83rkDU1Nan_qabare_dec
Token	eyJhbGciOiJIUzI1NiIsInR5c

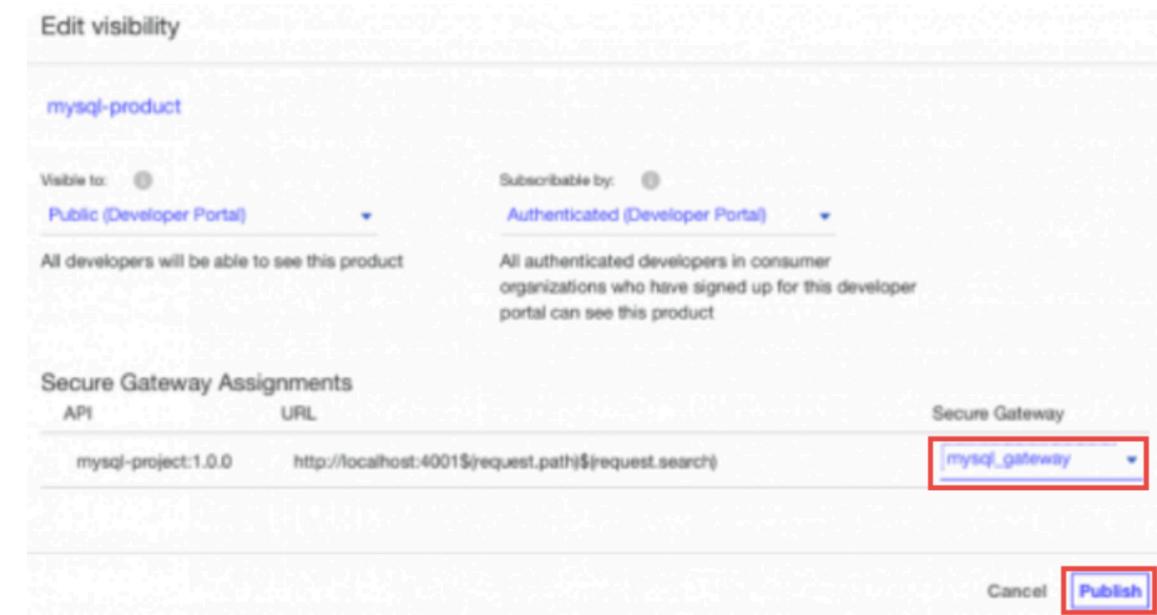
Using the secure gateway with your APIs

- When you have configured the secure gateway, you can use it with your APIs
- To use your secure gateway with APIs, complete the following steps:
 - Create your API and Product
 - In API Assemble view click the invoke policy to
 - open the invoke palette.
 - Select Access URL through Secure Gateway.
 - In the URL field, update the target-url with the
 - on-premises host name and port number.
- For example,
- **http://onpremdb2.rtp.raleigh.ibm.com:3055**
\$(request.path)\$(request.search)



Publishing API with secure gateway

- Select the staged Product.
Click Publish and select Secure Gateway Assignments. As a result, you have securely exposed your on-premises API to API Connect. Any TLS profiles that are associated with a destination are added. To check the TLS profiles, click Navigate to icon > Admin > Security > TLS Profiles. You can have multiple gateways for each API. You decide which gateway to use when you publish the API.



Testing your Secure Gateway

- After you have attached the gateway to an API, you can test the API to ensure that the gateway is working and that it produces the correct response.
- To test an API using the secure gateway:
 1. Click **Navigate to > Drafts > APIs > <Your API> > Assemble**.
 2. Click the **Explore** icon .
 3. Select an operation to invoke from the list provided.
 4. Provide Parameters if needed
 5. Click **Call Operation**.
 6. Review Response code and JSON

The screenshot shows the IBM Bluemix APIs interface. At the top, there's a navigation bar with 'Catalog', 'Support', and 'Manage' buttons. Below that, the 'notes 1.0.0' API is selected. The main area has tabs for 'All APIs', 'Design', 'Source', and 'Assemble'. The 'Assemble' tab is active. Under 'Explore', it says 'Sandbox catalog https://us.apiconnect.ibmcloud.com/orgs/soloveyusibmcom-dev/catalogs/sb'. It lists operations: 'POST /Notes', 'PUT /Notes', 'PATCH /Notes', 'GET /Notes' (which is selected and highlighted with a red box), and 'POST /Notes/replaceOrCre...'. Below these, there's a 'Parameters' section with a 'filter' field and a 'Call operation' button, which is also highlighted with a red box. To the right, the response is shown: 'Code: 200 OK', 'Headers: content-type: application/json x-global-transaction-id: 1560839', and a JSON object:

```
{  
  "actorId": 1,  
  "firstName": "PENELOPE",  
  "lastName": "GUINNESS",  
  "lastUpdate": "2006-02-15T04:34:33.000Z"  
}
```

Lab

IBM