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.

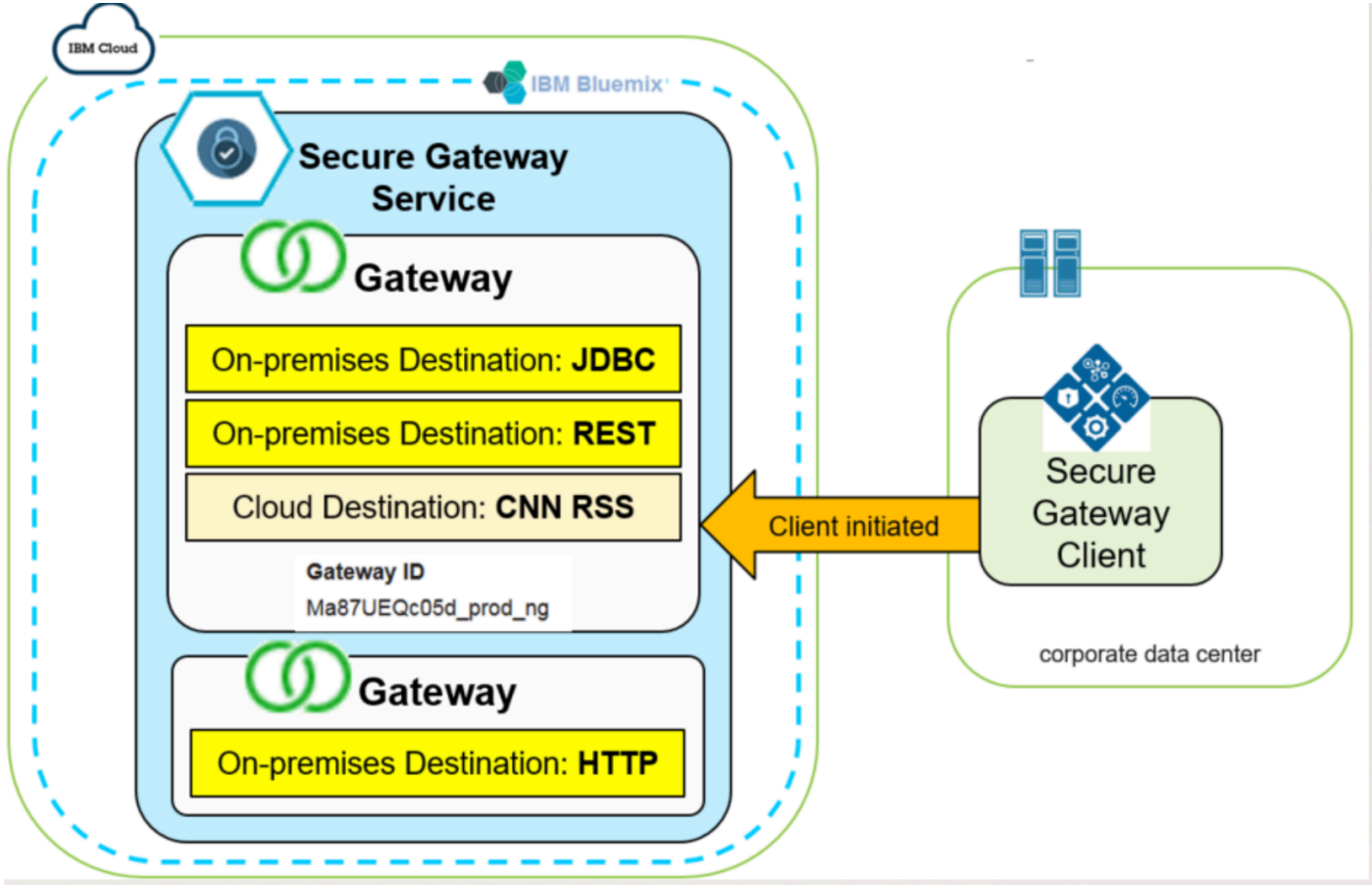
- Secure Gateway provides secure way to connect Bluemix applications to remote locations on-premises or in the cloud.

- https://console.ng.bluemix.net/docs/services/SecureGateway/secure_gateway.html

Secure Gateway Concept

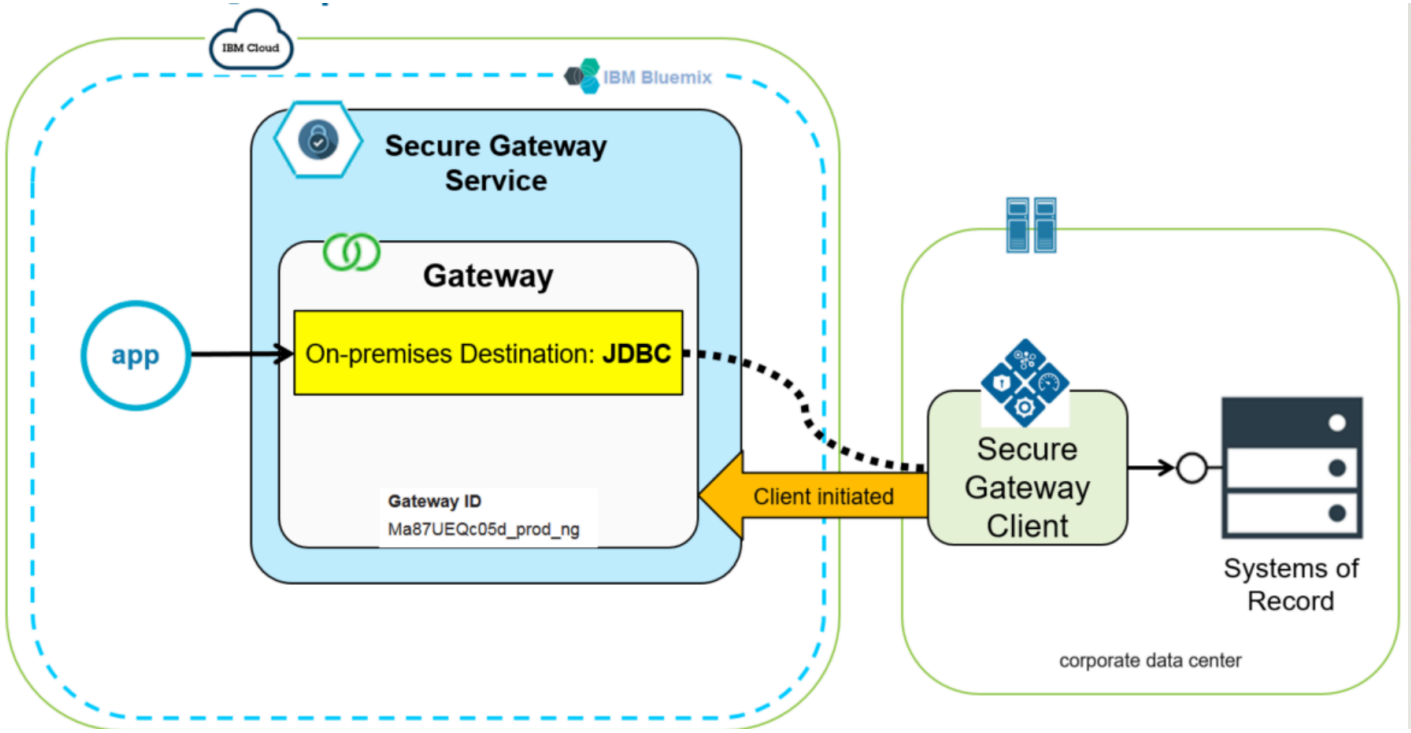
- In the secure gateway configuration, the Secure Gateway service defines one or more gateways. The gateways are identified by the Gateway IDs. The Secure Gateway client initiates connection to the Gateway based on the Gateway ID. The gateway ID contains the destination information.

- The secure gateway client runs on DataPower appliances or as a Node.js program.



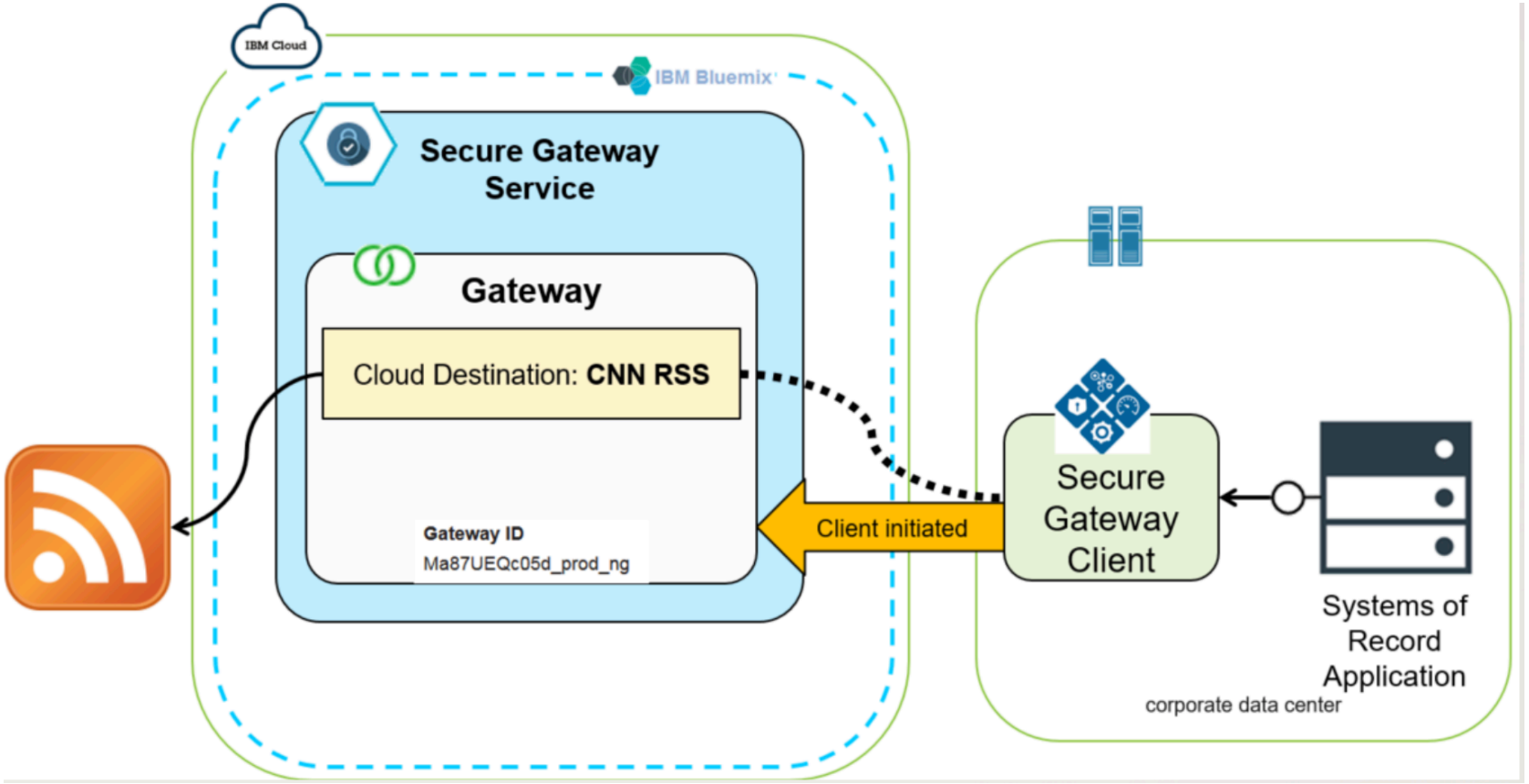
Secure Gateway on-premises destination

- 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.



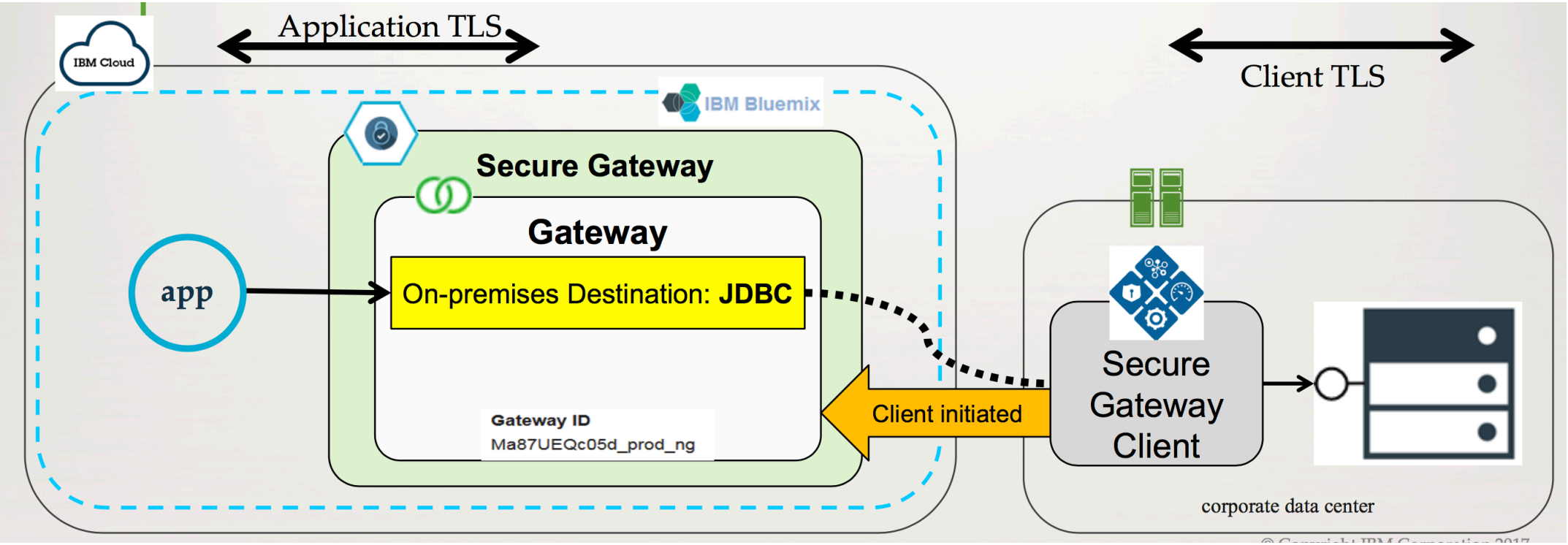
Secure Gateway cloud destination

- 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.



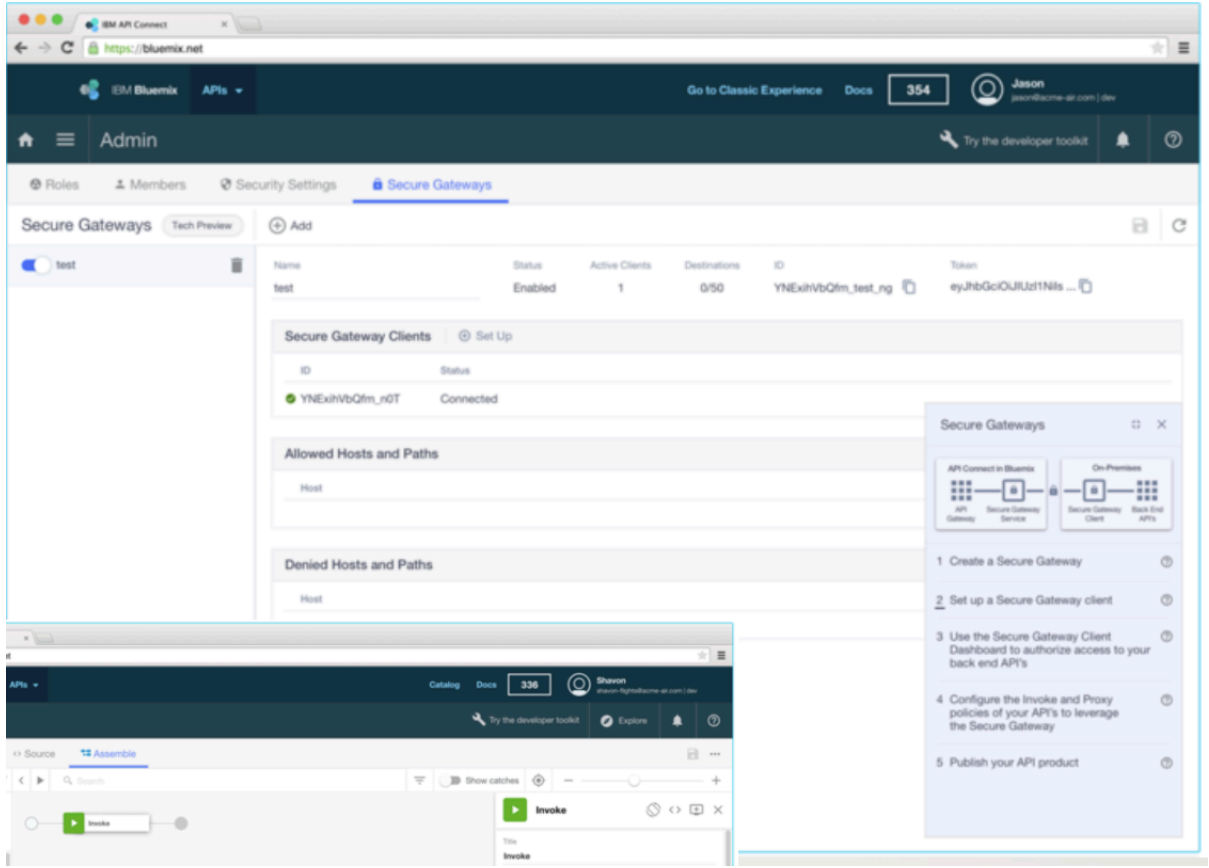
Security Overview

- 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.



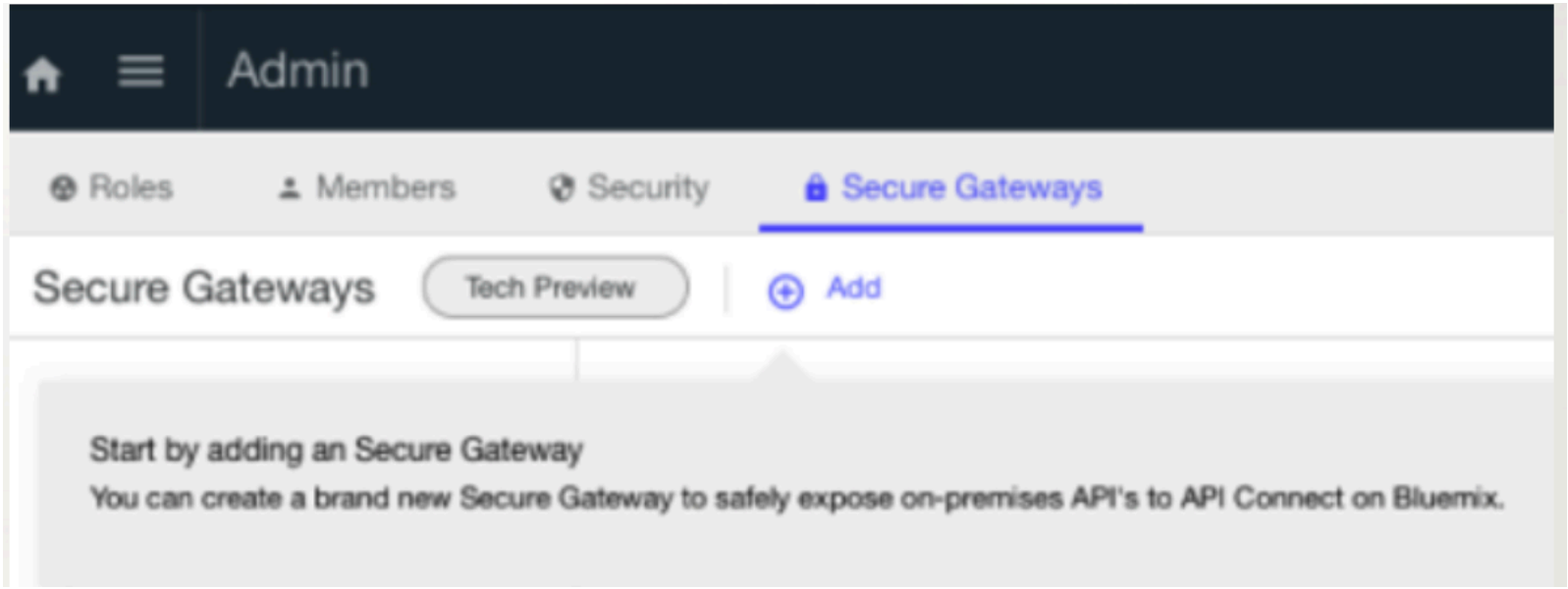
New Secure Gateway – APIC Integration

- **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



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

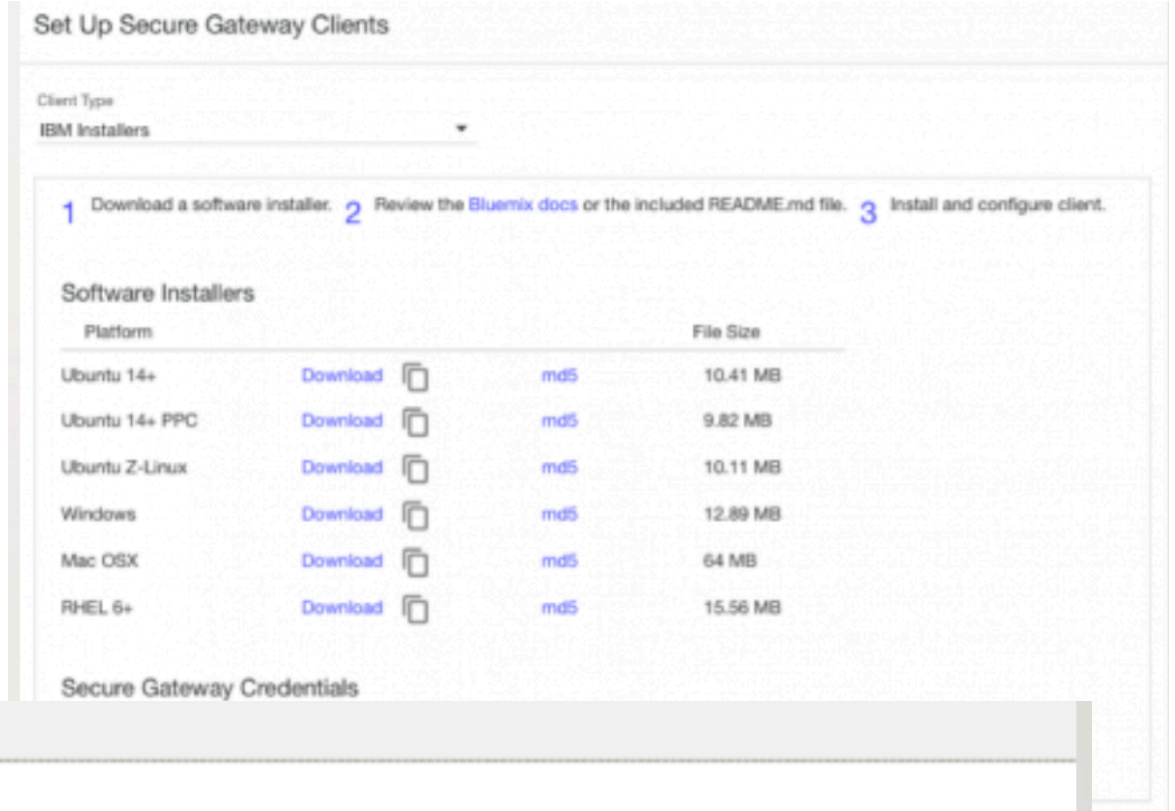


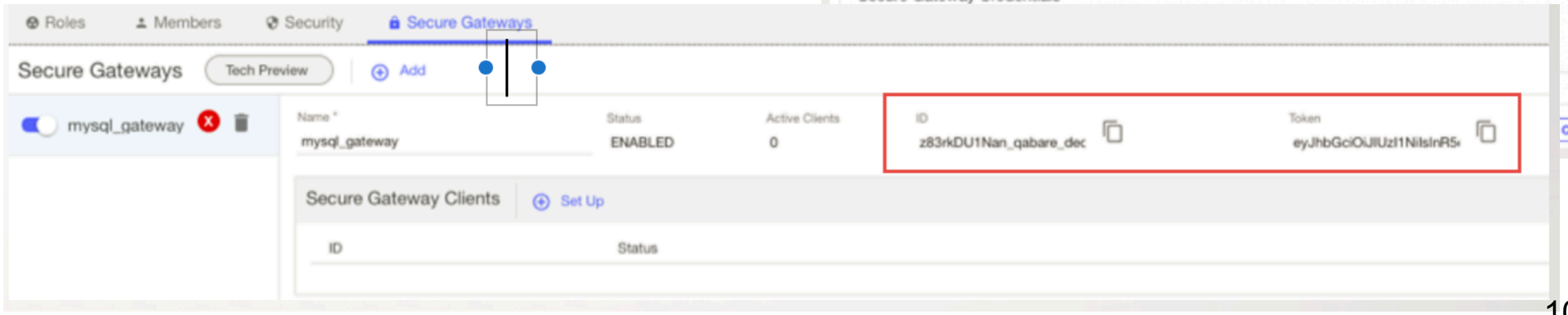
Exposing on-premises APIs through a secure gateway

- You can create a secure gateway to safely expose on-premises APIs to IBM® API Connect for BluemixTM
  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.

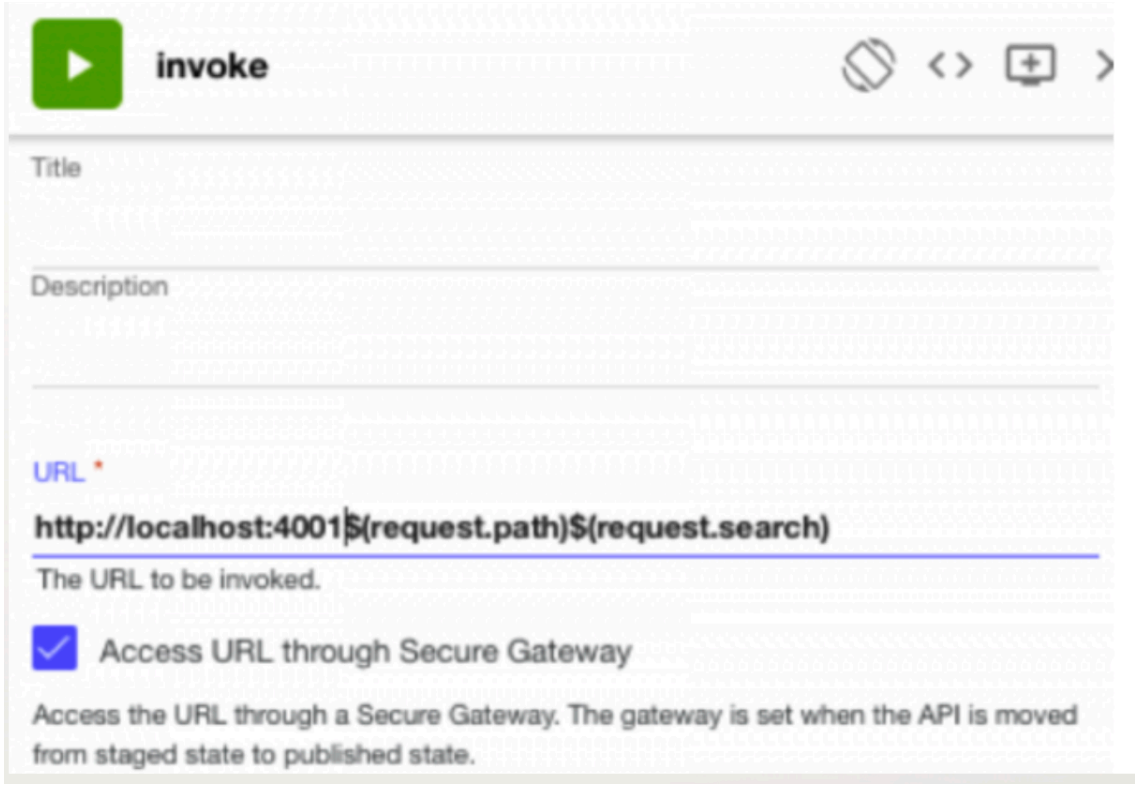




Using the secure gateway with your APIs

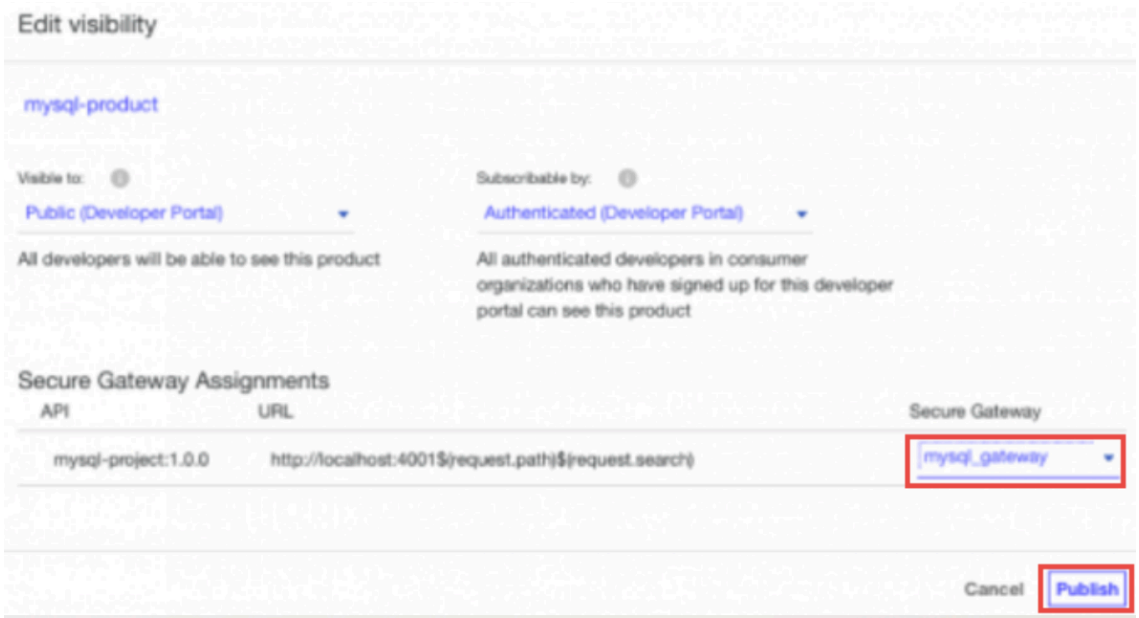
- When you have configured the secure gateway, you can use it with your APIs

- 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

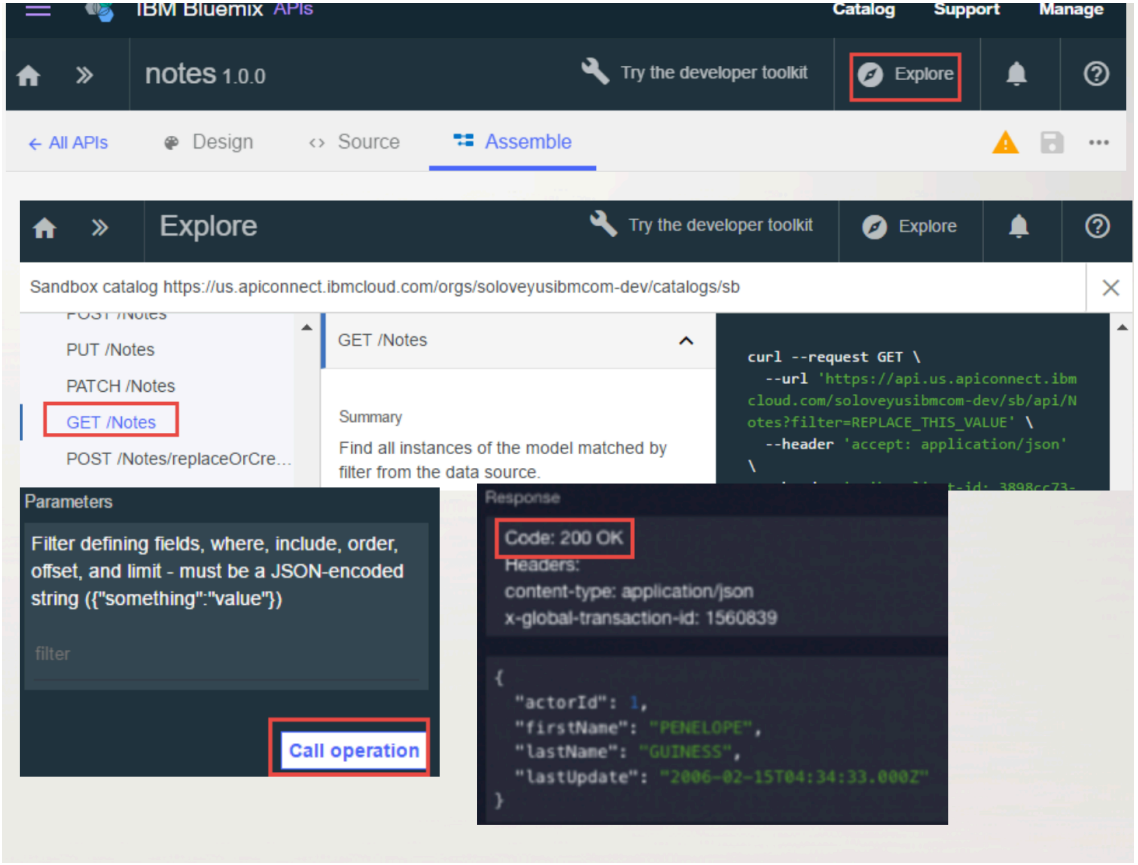
- Select the staged Product.
  Click Publish and select Secure Gateway Assignments. As a result, you have securely exposed your on- premises API to API Connect. Any TLS profiles that are associated with a destination are added. To check the TLS profiles, click Navigate to Navigate to icon > Admin > Security > 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



Lab