SAP Advanced Event Mesh - Security

SAP Advanced Event Mesh - Security

1. What you'll learn: Overview

- Fine-grained security access in AEM.

2. What you need: Prerequisites

- Complete all exercises to start up brokers in day 1.
  You access and use the same broker you setup previously.

3. Security and fine grained access control to topics

For this exercise and in general, we would like to take this opportunity to answer a common question:

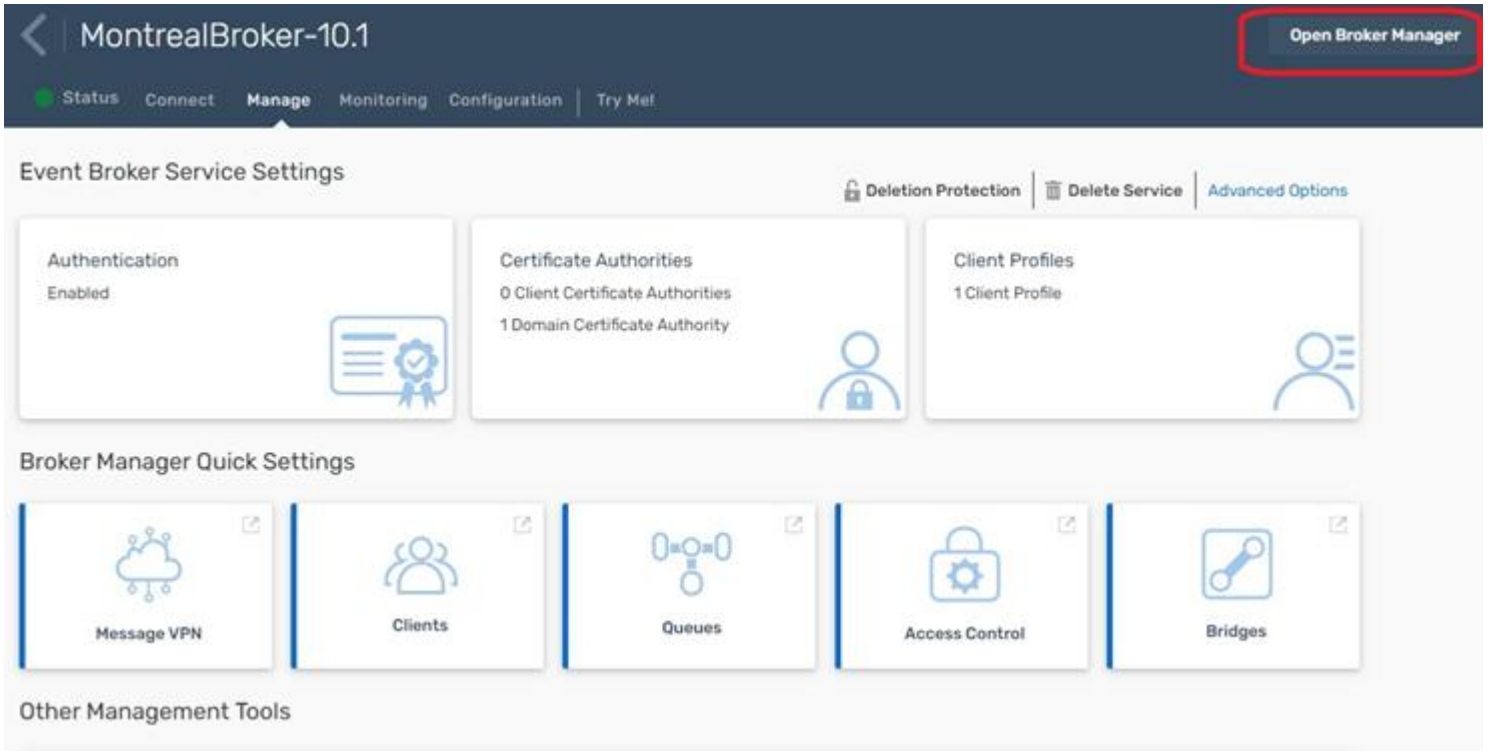
Is it possible to prevent clients from publishing to certain Topics and/or subscribing to certain topics?

The answer is absolutely!

We would like everyone to experience an Access Control List and how it can be used to control what is published or subscribed.

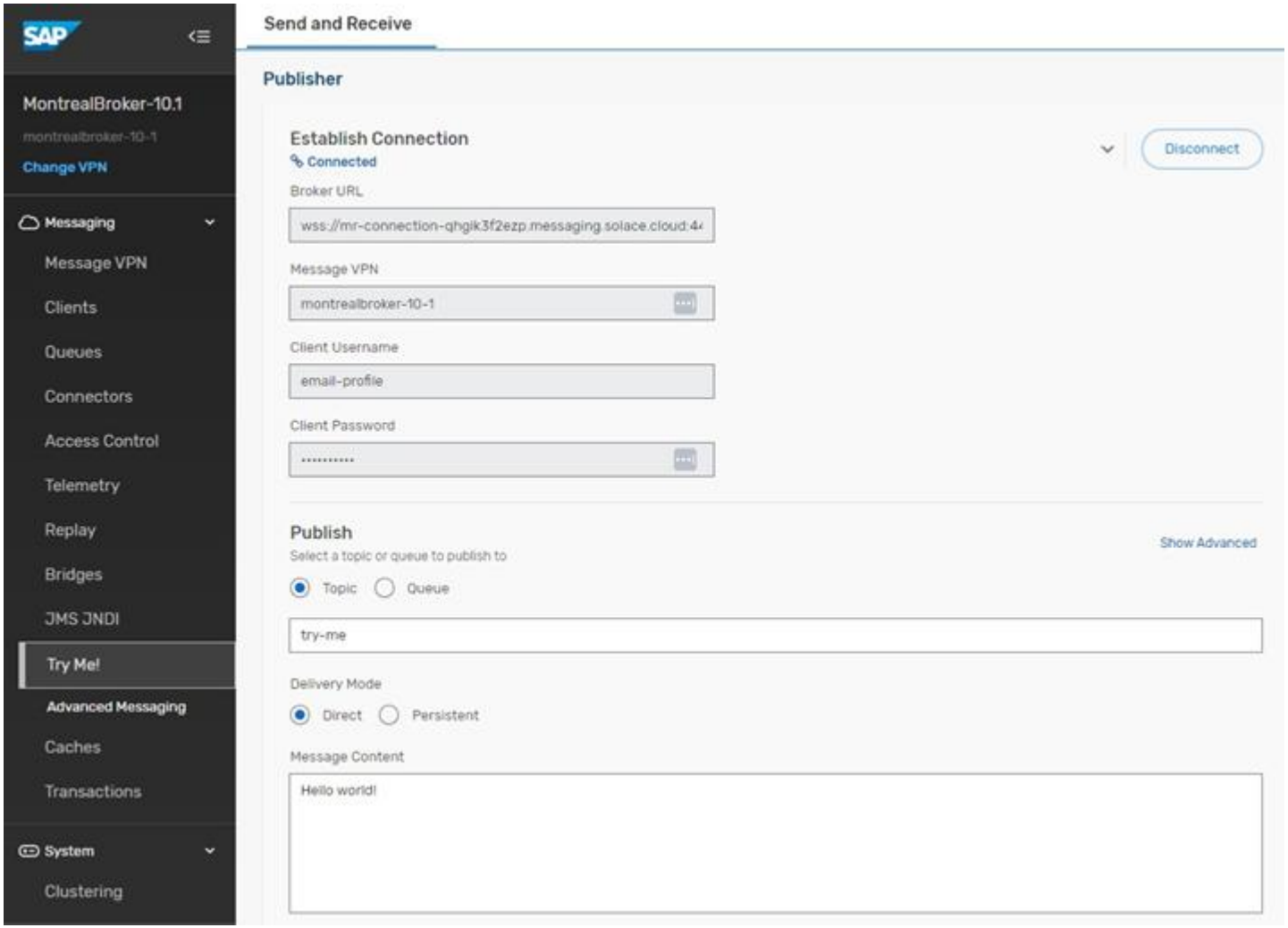
Experimenting publishing and subscribing to protected topics

From the **console**, we need to navigate to the **broker manager**. You can get there by either clicking on the "**Open Broker Manager**" button or clicking any of the Tiles labelled "**Clients**", "**Queues**", "**Access Control**".



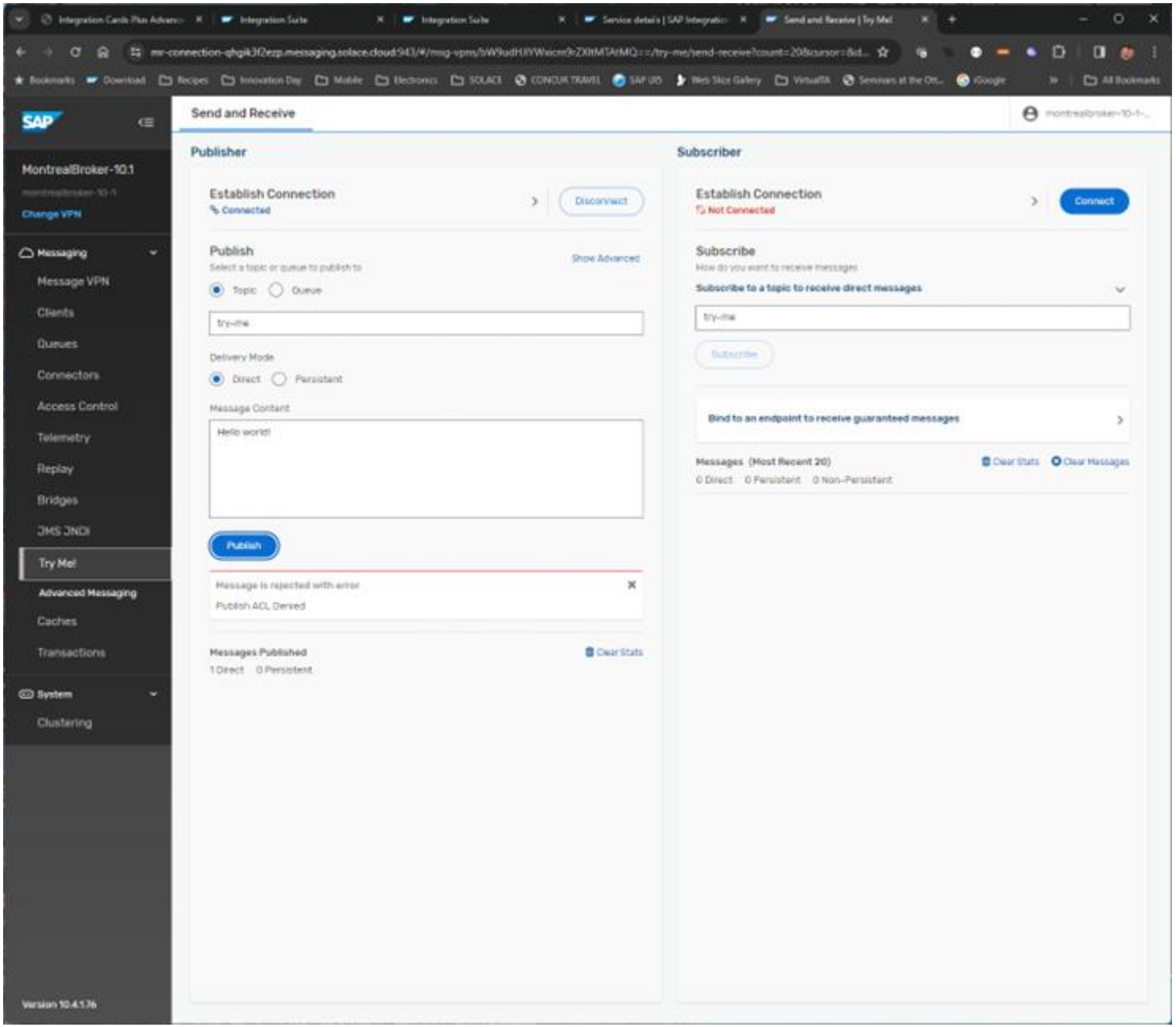
You will then see the **Broker Manager** Screen and on the left you will see a more advanced "**try-me**" test client. Click on it, to reveal the information you must provide to connect: For this screen, you will be trying to connect to our Broker where we have created an ACL to limit what you can do and on what topics you can publish. The information you will use is as follows:

```
Broker URL: wss://montrealbroker.messaging.solace.cloud:443
Message VPN: montrealbroker-10-1
Client UserName: email-profile
Client Password: ******** <- provided during the course
```

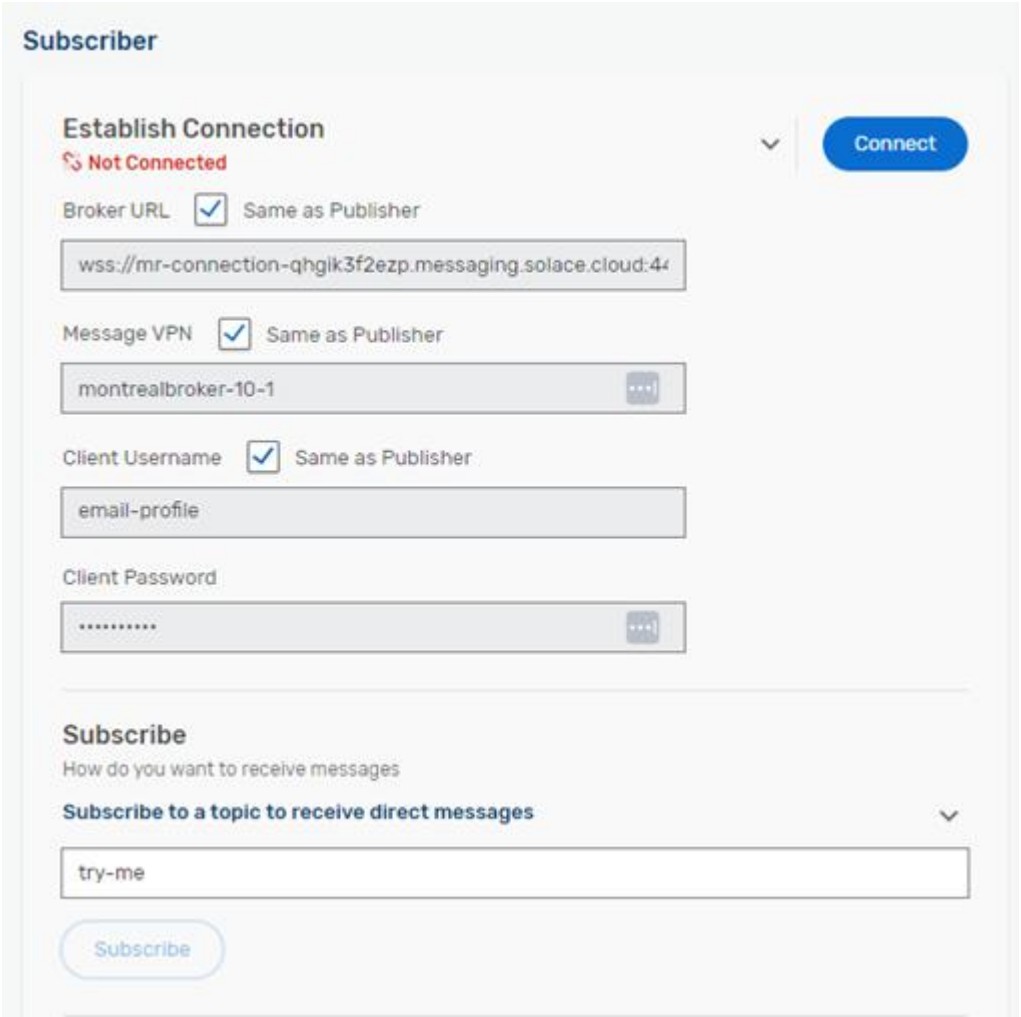


Once you have entered in the connectivity information, you should see the "Connected" message in blue.

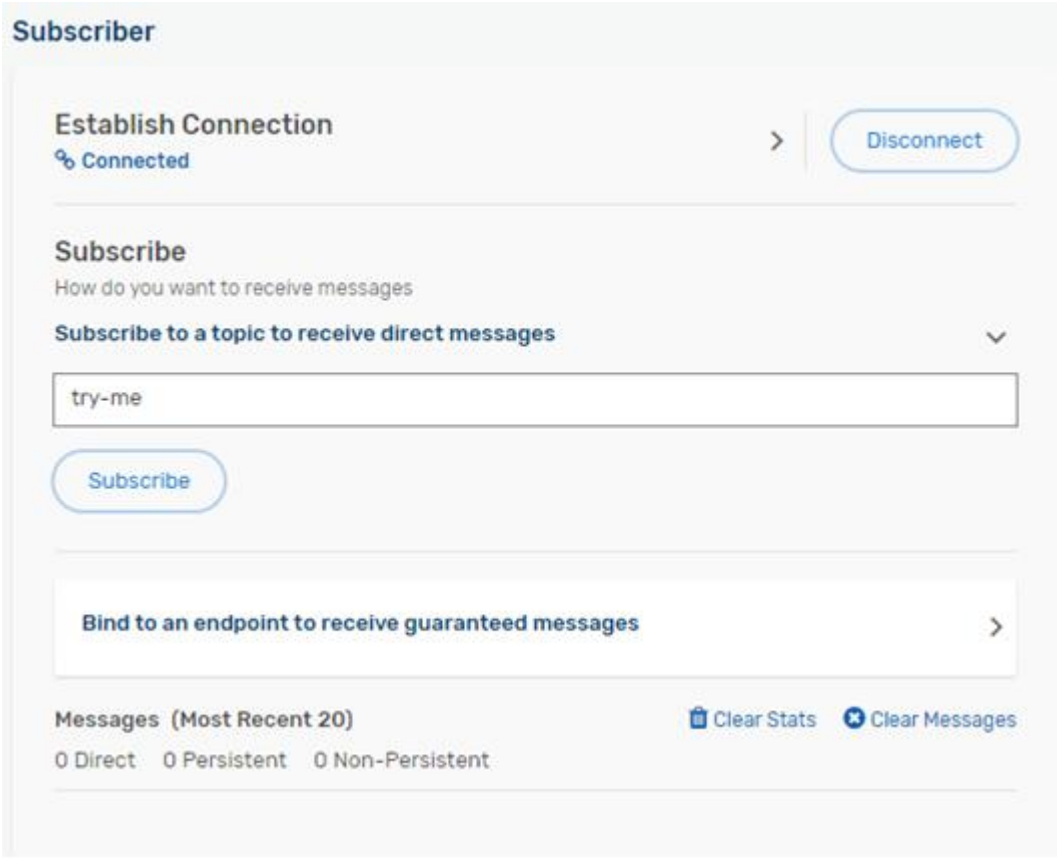
Once connected, change nothing and hit "**Publish**", you should immediately see the "**Publish ACL Denied**" on this action because the ACL will not permit you to complete this action.


Send and Receive
MontrealBroker-10.1
Change VPN
Messaging
Message VPN
Clients
Queues
Connectors
Access Control
Telemetry
Replay
Bridges
JMS JNDI
Try Me!
Advanced Messaging
Caches
Transactions
System
Clustering
Version 10.4.1.76
Publisher
Establish Connection
Connected
Disconnect
Publish
Select a topic or queue to publish to
Show Advanced
Topic
Queue
try-me
Delivery Mode
Direct
Persistent
Message Content
Hello world!
Publish
Message is rejected with error
Publish ACL Denied
Messages Published
1 Direct 0 Persistent
Clear Stats
Subscriber
Establish Connection
Not Connected
Connect
Subscribe
How do you want to receive messages
Subscribe to a topic to receive direct messages
try-me
Subscribe
Bind to an endpoint to receive guaranteed messages
Messages (Most Recent 20)
Clear Stats
Clear Messages
0 Direct 0 Persistent 0 Non-Persistent

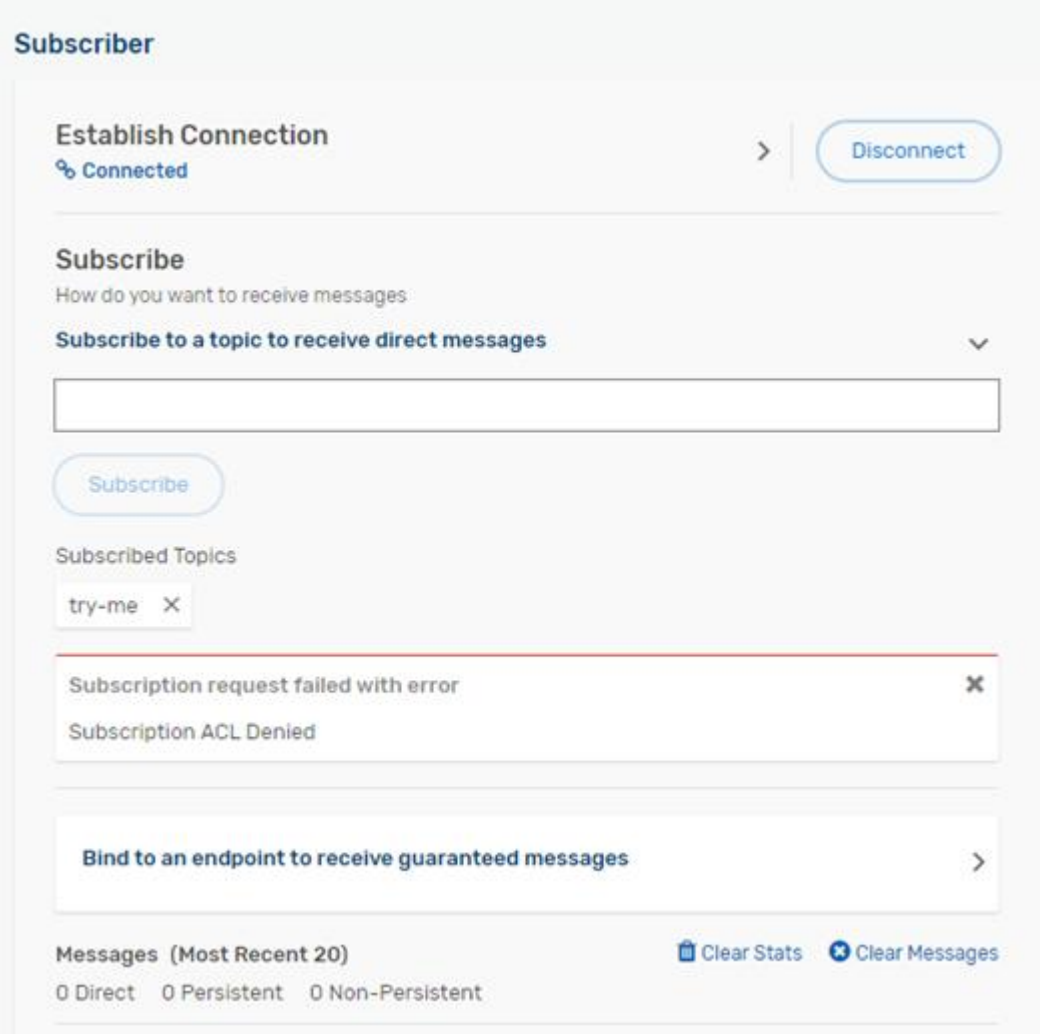
Now, let's try the exact same thing with the subscription. Hit the "**Connect**" button, and you should see the connection properties already populated so accept this and hit connect.



Once connected, you will see this:



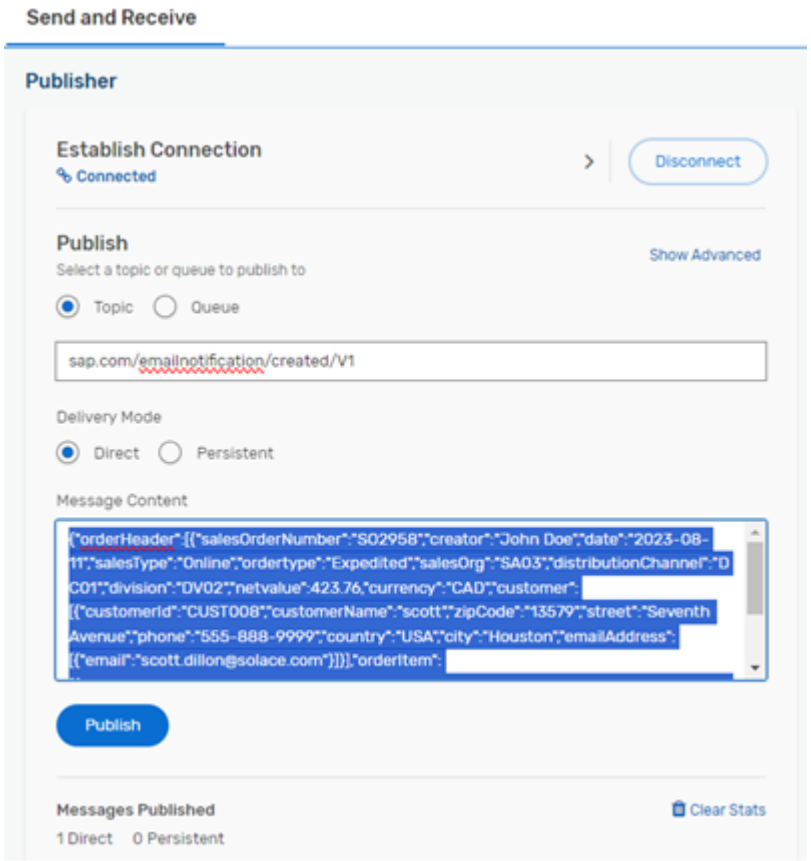
From here, just hit the **Subscribe** button and you should see the following screen:



Again, you have been "**Denied**" - That was expected. 😊

Now, let’s head back to the "Publisher" and change the "Topic" to `sap.com/emailnotification/created/V1` Use the following structure for your Message Content....be sure to copy the entire structure below including all of the curly braces. This is the structure that is passed to the Solace Event Mesh for processing. If successful, you should receive an email shortly after publishing with the information contained in the message. In the structure below, please replace "**YOUREMAILADDRESS**" with your actual email address prior to hitting the publish button.

```
{"orderHeader": [{"salesOrderNumber":"SO2958","creator":"John Doe","date":"2023-08-
11","salesType":"Online","ordertype":"Expedited","salesOrg":"SA03","distributionChannel":"DC01",
"division":"DV02","netvalue":423.76,"currency":"CAD","customer": [{"customerId":"CUST008",
"customerName":"scott","zipCode":"13579","street":"Seventh Avenue", "phone":"555-888-
9999","country":"USA","city":"Houston", "emailAddress":[{"email":"YOUREMAILADDRESS"}]}],
"orderItem":[{"item":"ITEM013","material":"MAT013", "materialType":"Product",
"itemType":"Standard","itemDescription":"Volt Electric bike",
"orderSchedule":[{"scheduleNumber":"SCH013","quantity":40, "uom":"EA"}]}]}]}
```

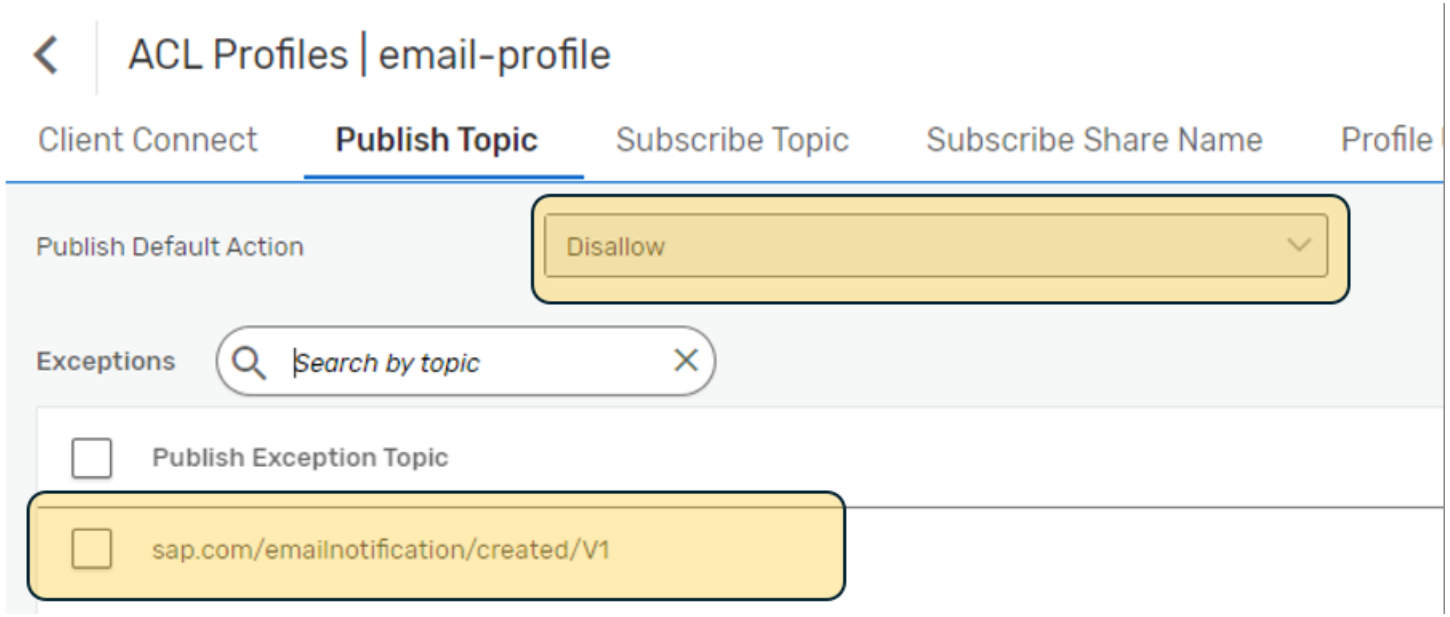


If you have entered the topic and message body correctly, you should see that 1 message has been published.

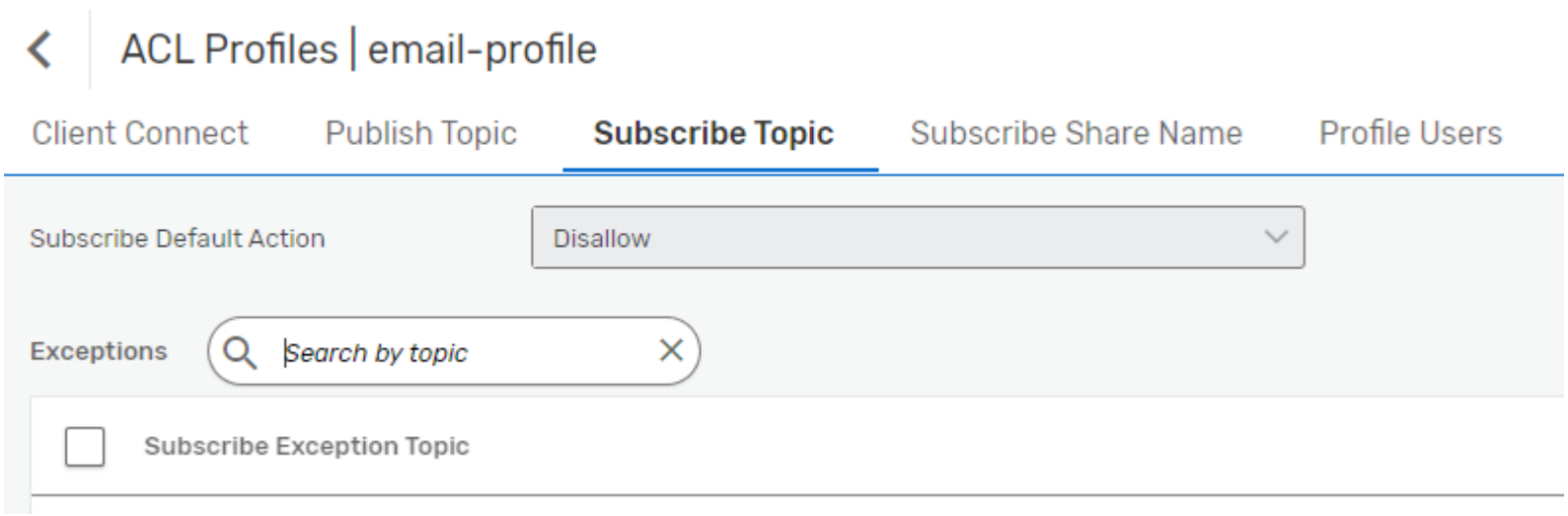
So how did we do that? The magic happens in the ACL Profile as shown next.

Broker Topic ACLs

We have changed the Default Publish Action to be Disallow. In other words, unless we specify an exception, the user profile associated with this ACL cannot publish anything by default. In this case, as you can see, we have listed one exception.



For the subscription settings, it's very simple: We specify the Default Action is "Disallow" and do not provide any exceptions. AKA, this ACL does not permit any subscriptions.



Now that you have this understanding, you will see that this ACL profile could be used for a client that is only allowed to send EmailnotificationCreated events on the specified topic. Everything else is prohibited by the email-profile user ACL, so it can only be used for this single purpose.

As you can see, broker ACLs are a quite powerful tool to tightly control access to the broker and its topics. You can separately control publish topics and subscribe topics and even IP address ranges that clients are allowed to connect from. In addition to topic ACLs, remember that queue access is controlled by the queue ownership model and the "other permission".

11. Takeaways

✅ How fine-grained security access in AEM works.

Thanks for participating in this codelab! Let us know what you thought in the Solace Community Forum! If you found any issues along the way we'd appreciate it if you'd raise them by clicking the Report a mistake button at the bottom left of this codelab.