SecurePost Listener ('Cloud' Mode)

Version 1.5.17

November 11, 2020

1stMILE, LLC
8383 158th Ave NE, Suite 100
Redmond, WA 98052

www.1stmile.com

© 2019-2020 1stMILE, LLC. All rights reserved.

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in Merchant Partners product. You may copy and use this document for your internal, reference purposes.

© 2019-2020 1stMILE, LLC. All rights reserved.

All trademarks are property of their respective owners.

Contents

Copyright 1
Contents 2
Overview 3
Communicating with SecurePost Listener 4
Development/Production 4
Request Authorization 5
Device ID 7
WebSocket Communication 9
Name-Value Pairs 9
JSON 11

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

Overview

The 'Cloud' mode of the SecurePost Listener provides integrators the capability of communicating the SecurePost Listener over the web outside of their local network. POS applications open a WebSocket connection with a Client Routing Service, which forwards data written into the WebSocket to the appropriate SecurePost Listener instance. After processing the request, SecurePost Listener sends the response back to the Client Routing Service, which finally writes the response back to the WebSocket for the POS application to receive.

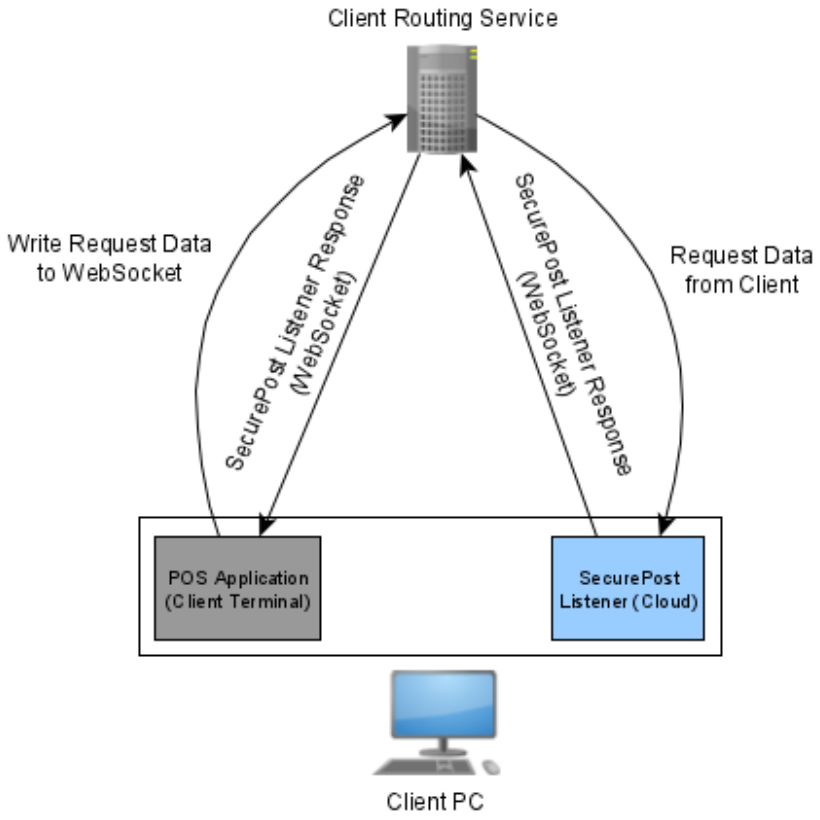


Figure 1: POS Application communicates to the Client Routing Service.

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

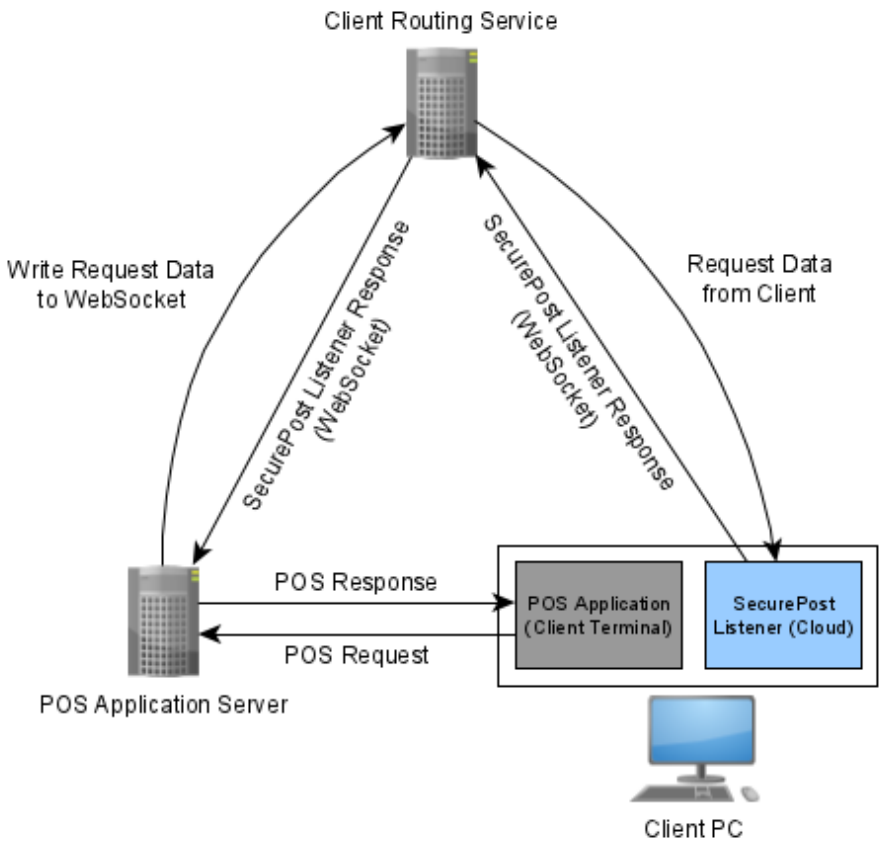


Figure 2: POS Application Server communicates to the Client Routing Service.

Communicating with SecurePost Listener

POS applications must obtain an access token (JWT access_token) and a device ID (unique to each installation) prior to establishing the WebSocket connection.

For more information about WebSockets, refer to https://en.wikipedia.org/wiki/WebSocket or https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API.

Development/Production

Integrators must obtain credentials and test account information from 1stMILE. During integration, development credentials and endpoints must be used. Once the integration is certified, production credentials and endpoints must be used.

- Username and Password

  These values identify the ISV and are required in the JSON payload to obtain the JWT.

- Client ID and Client Secret

  These values are used in the HTTP Basic Authentication header to identify the ISV.

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

- Test Account ID, Sub ID and Merchant PIN

  These values identify a test merchant that may be used in SecurePost Listener for testing purposes.

- To use SecurePost Listener in development mode, you must manually edit the listener.xml file. Manual editing should be performed with a text editor such as Notepad. This file can be found in the following folder:

  %APPDATA%\Innuity\ATSSecurePostUILib

  Add the highlighted "UseDev" line as shown below:

```
    ...
    <setting name="UseLocalComm" value="0" />
    <setting name="MPSignal" value="0" />
    <setting name="UseDev" value="1" />
  </SecurePostListener>
</configuration>
```

- To use SecurePost Listener in production mode, simply remove the "UseDev" line described above, or change the value from "1" to "0".

Request Authorization

POS applications must obtain a JWT access token to initiate communication. Using the standard HTTP Basic Access Authentication, clients must include client_id and the client_secret in the HTTP Header along with a JSON payload containing the username, password, scope, and grant_type. Below is an example:

Method: POST

Development endpoint: https://transmp03.merchantpartners.com/fm/oauth/token

Production endpoint: https://processing.1stmile.com/fm/oauth/token

HTTP Basic Access Authentication Header:

Authorization: Basic BASE64_ENCODED("client_id:client_secret")

Content-type: application/json

Accept: application/json

Sample Request:

```
{
  "username": "xxx@example.com",
  "password":"******************",
  "scope":"default"
}
```

Sample Response:

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

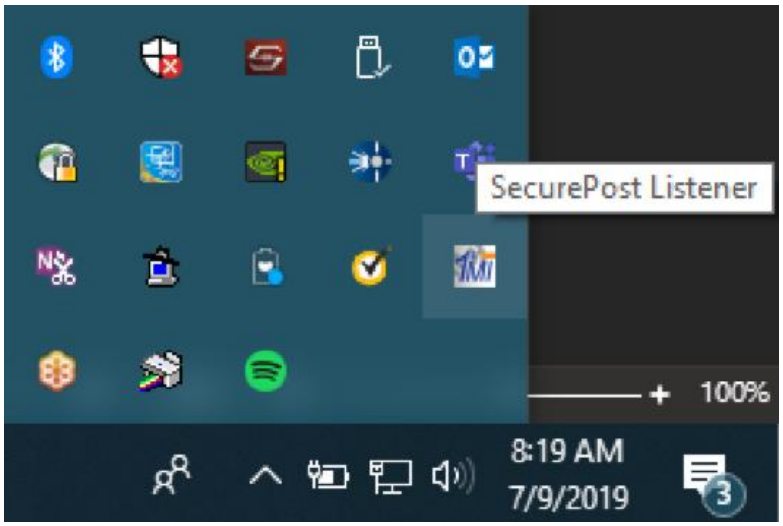
```
{
   "scope":["client"],
   "client_id":"1001",
   "user_allowed_locations":[],
   "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ0b2tlbl90eXBlIjoiQmVhcmVy
                    IiwianRpIjoiWFBBTXJDVHRBN2JpVFVNZGlETW5wd0FBQU5rIiwic2NvcGUiOlsiY2
                    xpZW50Il0sImNsaWVudF9pZCI6IjEwMDEiLCJzaWQiOiJjNTc2MGQ0YjkwMDU0MzRm
                    YTA5Mjk5NmRmMGJjYjViYmE0NDUzYjcwN2ZlN2FmMTY0MmM3ZjBiYjYyNDFiNDExIi
                    wiaXN2IjoiMTAwMSIsImlhdCI6MTU1OTIzNTc1NiwiZXhwIjoxNTU5Mjg5NTc2fQ.-
                    IiZbmlcME4pktfejgOfpvWX_uByfS7z9wMAxhSfBjw"
}
```


Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

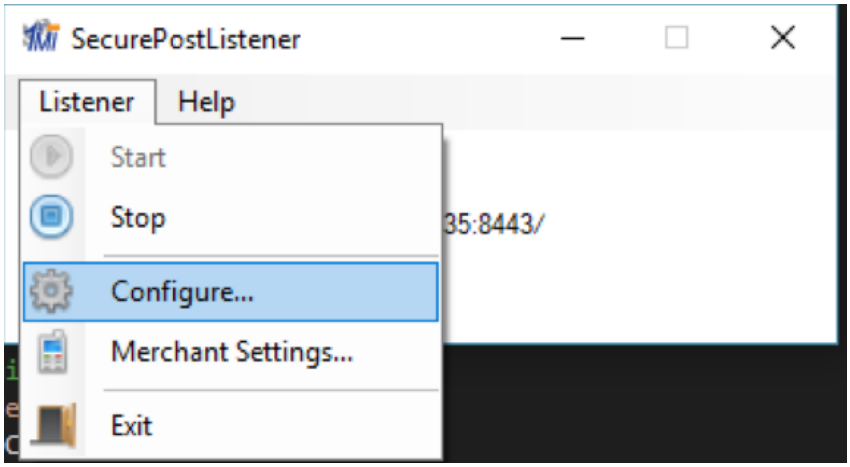
Device ID

In addition to the access token, to communicate with SecurePost Listener installed on a specific workstation, the POS application must obtain SecurePost Listener's device ID. The device ID, which is unique to every installation, will be used as the serial number when making the initial GET request for communication. The device ID can be found by completing the following:

1. Launch SecurePost Listener.
2. Open the SecurePost Listener dialog from the system tray.

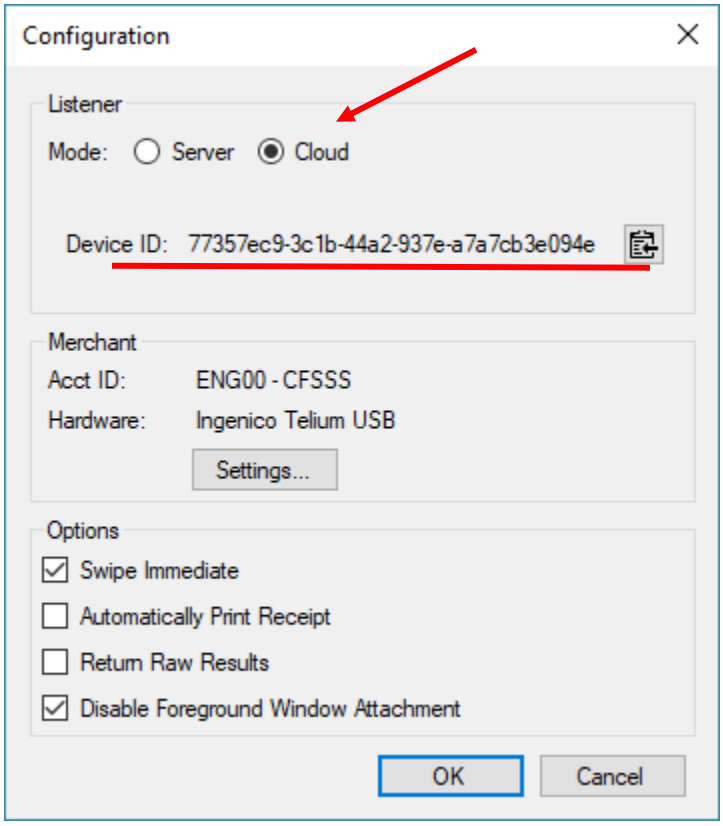


3. Open the configuration.

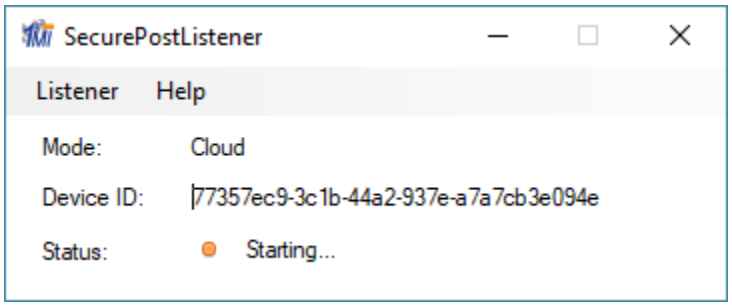


Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

4. Change the mode to 'Cloud' (if not set already)



If the SecurePost Listener is already configured for 'Cloud', the serial number will appear on the initial dialog:



Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

WebSocket Communication

Using the WebSockets API, you would establish a connection with the endpoint listed below, send data to the server, and wait for messages to be returned by the server.

Establish the WebSocket connection with one of the following URLs depending on whether your application has been certified or not:

Development URL:

wss://transmp03.merchantpartners.com:8443/logon?serialnum=*DEVICE_ID*&accesstoken=*ACCESS_TOKEN*

Production URL:

wss://processing.1stmile.com/logon?serialnum=*DEVICE_ID*&accesstoken=*ACCESS_TOKEN*

Replace *DEVICE_ID* and *ACCESS_TOKEN* with the appropriate values.

With the WebSocket connection established, there are two ways in which data can be written: Name-Value Pairs or JSON.

Name-Value Pairs

Data should be sent as URL encoded name-value-pairs separated by an ampersand.

The following sample shows a request for a credit card sale in the amount of $1.25 to be processed and its response after it has been processed.

Sample Request:

```
PaymentType=Credit&TransactionType=Sale&Amount=1.25&MerchantOrderNumber=20110511-1109
```

Sample Response:

```
Result=Accepted
AuthCode=SALE:TEST:::1303704478:N::U
OrderID=1047317610
TransactionID=1303704478
AccountNumber=XXXXXXXXXXXX5454
Amount=1.25
Expiration=05/2022
Name=Mp Tester
PayType=MasterCard
EntryMethod=KEYED
```

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

Request Parameters

The following request parameters are supported.

PaymentType

The PaymentType parameter specifies the payment type. Valid values are listed below. If this parameter is not provided, the default value of 'Credit' will be used.

Value	Description
`Credit`	Credit or Debit card transaction.
`Check`	ACH transaction.

TransactionType

The TransactionType parameter specifies the type of transaction to process. Valid values are listed below. If this parameter is not provided, the default value of 'Sale' will be used.

Value	Description
`Sale`	Perform a sale.
`PreAuth`	Perform an Authorization only transaction. This value is only valid when PaymentType is 'Credit'.
`PostAuth`	Perform a Post (Capture) transaction. This value is only valid when PaymentType is 'Credit'.
`Refund`	Perform a Refund for a previously executed Sale or Authorization.
`Void`	Void a credit card authorization or sale.
`CreditApplication`	Perform a credit application or credit application action.
`AccountLookup`	Perform an account lookup.
`TokenLookup`	Perform a tokenized account lookup.
`SigCap`	Perform a stand-alone signature capture.
`GiftCard`	Perform a gift card action specified in the GiftCardAction parameter.
`TransactionSearch`	Perform a Transaction Search operation.
`TextToPay`	Generate a pay link for the consumer to pay for a transaction.

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.

`TextToAuthorize`	Generate an authorization for the consumer to authorize a work order.

For more details regarding request parameters, please refer to the I_first_mile_middleware_guide.pdf found on the Merchant Partners documentation page.

JSON

Data should be sent as valid JSON. Refer to the 1stMILE MiddleWare Integration Guide for specifications of all supported JSON request payloads and their corresponding responses.

The following sample shows a request for a credit card sale in the amount of $1.25 to be processed and its response after it has been processed.

Sample Request:

```
{
    "transactionType": "Sale",
    "transaction": {
        "amount": 1.25,
        "merchantOrderNumber": "20200821-1101"
    }
}
```

Sample Response:

```
[{
        "status": "SUCCESS",
        "receiptGroup1": {
            "transactionType": "SALE",
            "transactionID": "1542240848",
            "transactionResult": "APPROVED",
            "account": "XXXXXXXXXXXX5454",
            "timestamp": "8/21/2020 10:02:07 AM",
            "merchantOrdernumber": "20200821-1101",
            "amount": 1.25,
            "entryMethod": "KEYED",
            "accountType": "MasterCard",
            "name": "James D. Customer",
            "orderID": "1253405302",
            "authCode": "TEST",
            "refCode": "1542240848-TEST",
            "avsResult": "N",
            "cvv2Result": "M"
        },
        "additionalDetails": {
            "expiration": "12/2020",
            "last4digits": "5454",
            "message": "Sale"
        }
    }
]
```

Copyright © 2019-2020 Merchant Partners, LLC
Proprietary and Confidential Information. Unauthorized reproduction or distribution prohibited.