Payment Simulator Tool Guide

Version: 1.0

28 July 2025

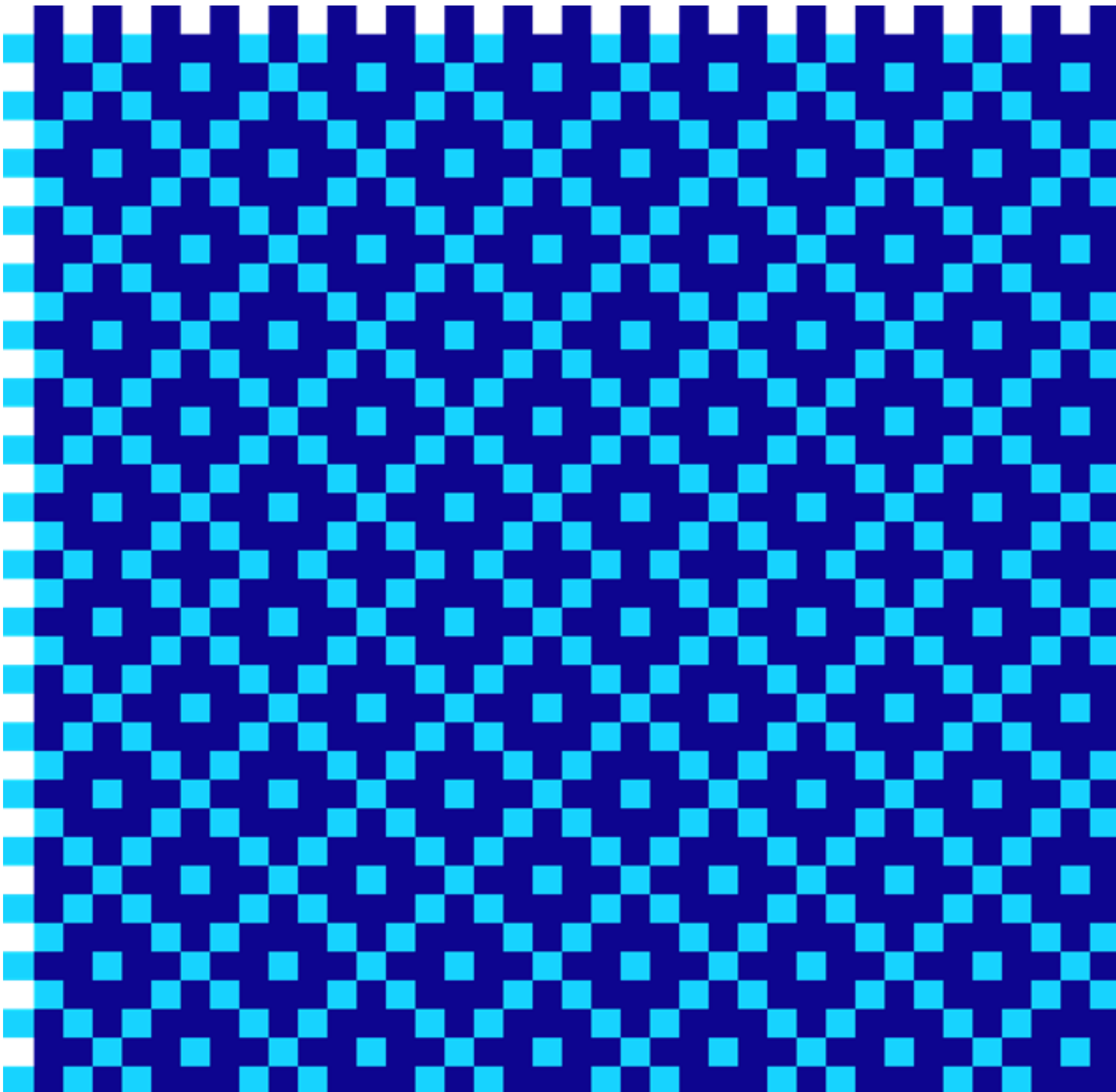
Publication number: PST-1.0-7/28/2025

For the latest technical documentation, see the Documentation Portal.

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682



Copyright

About this Guide

The Payment Simulator Tool is a comprehensive solution that enables clients to confidently launch and manage payment programs with ease and speed. The tool allows seamless end-to-end testing of API configurations, card processing rules, payment interfaces, and critical system integrations–all while minimising customer impact and enhancing operational efficiency.

Target audience

This guide is aimed at Program Managers and developers who want to test the integration of their systems and validate the setup of the External Host Interface (EHI) before going live in a production environment.

What's changed?

If you want to find out what's changed since the previous release, see the Document History section.

Other Documentation

Refer to the table below for a list of other relevant documents that should be used together with this guide.

Document	Description
EHI Guide	Describes the Thredd External Host Interface (EHI) and provides specifications on how to process and respond to messages received from EHI.
Smart Client Guide	How to use Smart Client, which is an administration application that can be used to view and manage cards and transactions in your programme.
Cards API Website	Describes how to use the Thredd REST-based API to send requests to Thredd.
Thredd Portal Guide	Describes how to use Thredd Portal, Thredd's new web application for managing your cards and transactions on the Thredd Platform.

Tip: For the latest technical documentation, see the Documentation Portal.

1 Getting Started

The Payment Simulator Tool is a comprehensive solution that enables clients to confidently launch and manage payment programs with ease and speed. The tool allows seamless end-to-end testing of API configurations, card processing rules, payment interfaces, and critical system integrations—all while minimising customer impact and enhancing operational efficiency.

Sign In to Payment Simulator Tool

To sign in to the Payment Simulator Tool:

1. Navigate to https://payment-test.uat.thredd.cloud/
2. Use the SSO to sign in. Contact Thredd to set up your SSO if it hasn't been set up already for Payment Simulator Tool.

Payment Simulator Tool Dashboard

The dashboard displays after successfully logging in to the Payment Simulator Tool. From the dashboard you can run tests and configure settings.

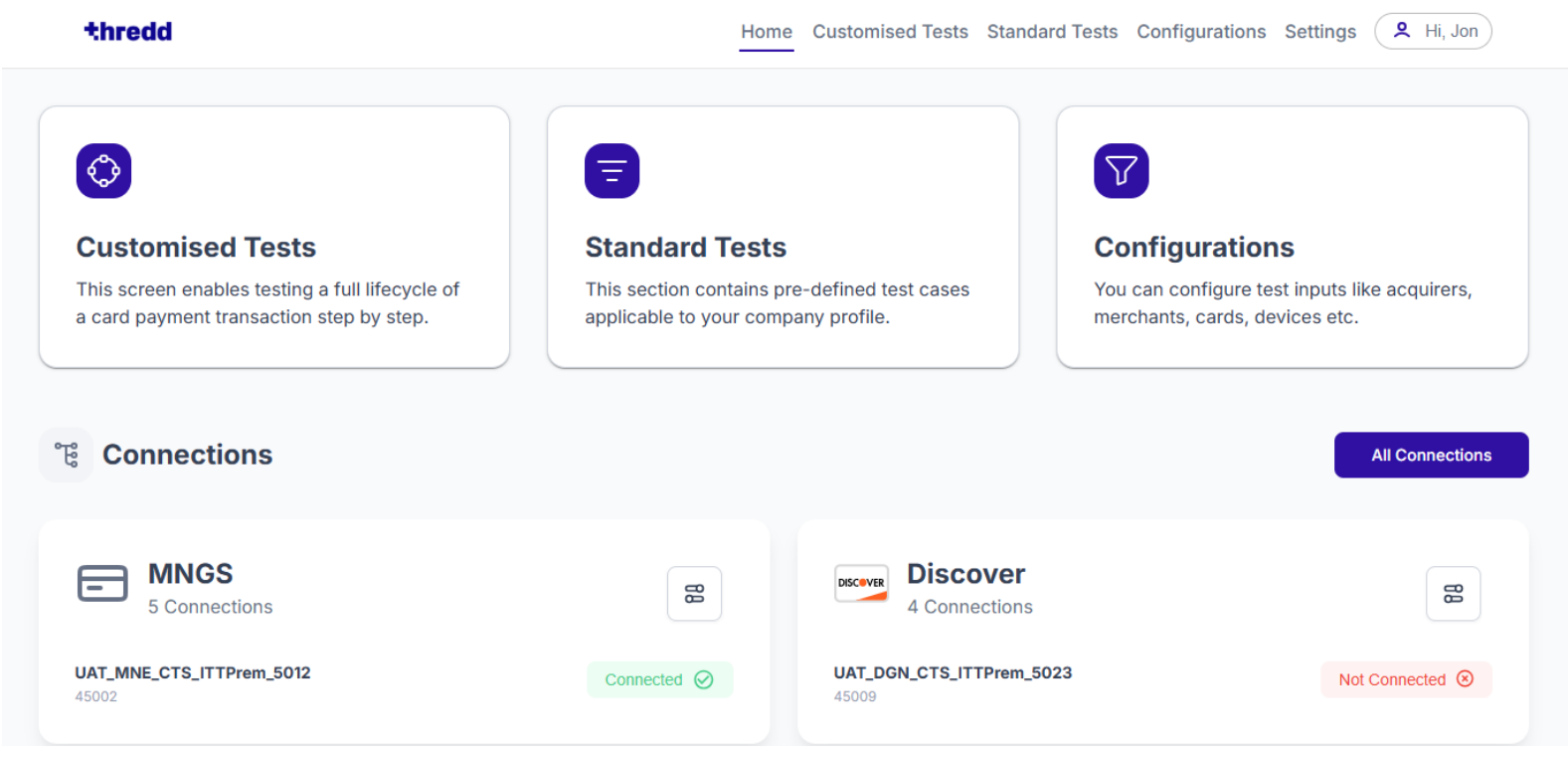


Figure 1: Payment Simulator Tool Dashboard

The top of the page consists of the following options:

- The Home option enables you to use shortcuts for running tests and configuring settings
- The Customised Tests option enables you to test a full lifecycle of a card payment transaction and create test cases
- The Standard Tests option enables you to test pre-defined test case applicable to your company
- The Configurations option enables you to configure test inputs for cards
- The Settings option enables you to create and manage user accounts

2 Settings

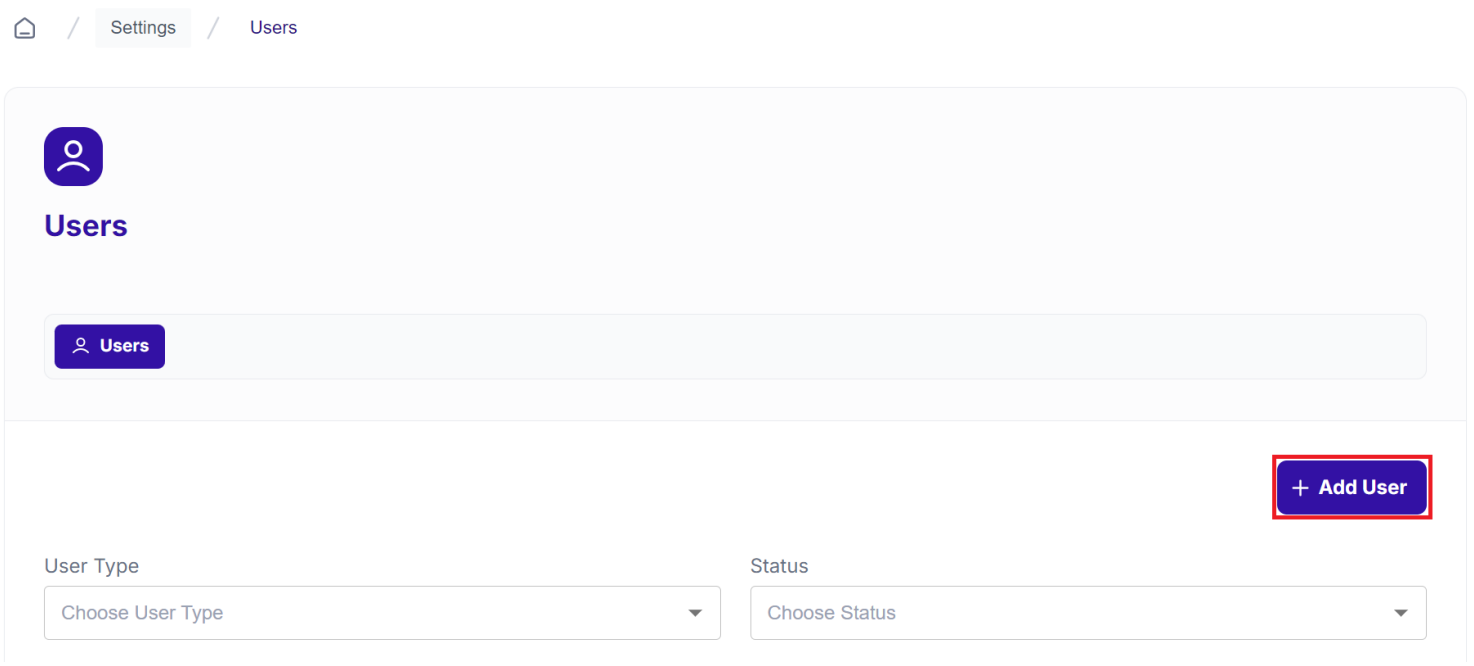
This section describes how to add a new user to the system on the Payment Simulator Tool. User management is an essential administrative task, enabling system administrators to control who has access to various parts of the tool by assigning appropriate roles.

Note: You must have the Admin role to be able to use the settings page. Users with a User role can only see the User Management section.

Add a New User

To add a new user:

1. Click **Add User**.



2. Enter the details for the new user in the required fields, such as the user's name, email address, and other essential information.

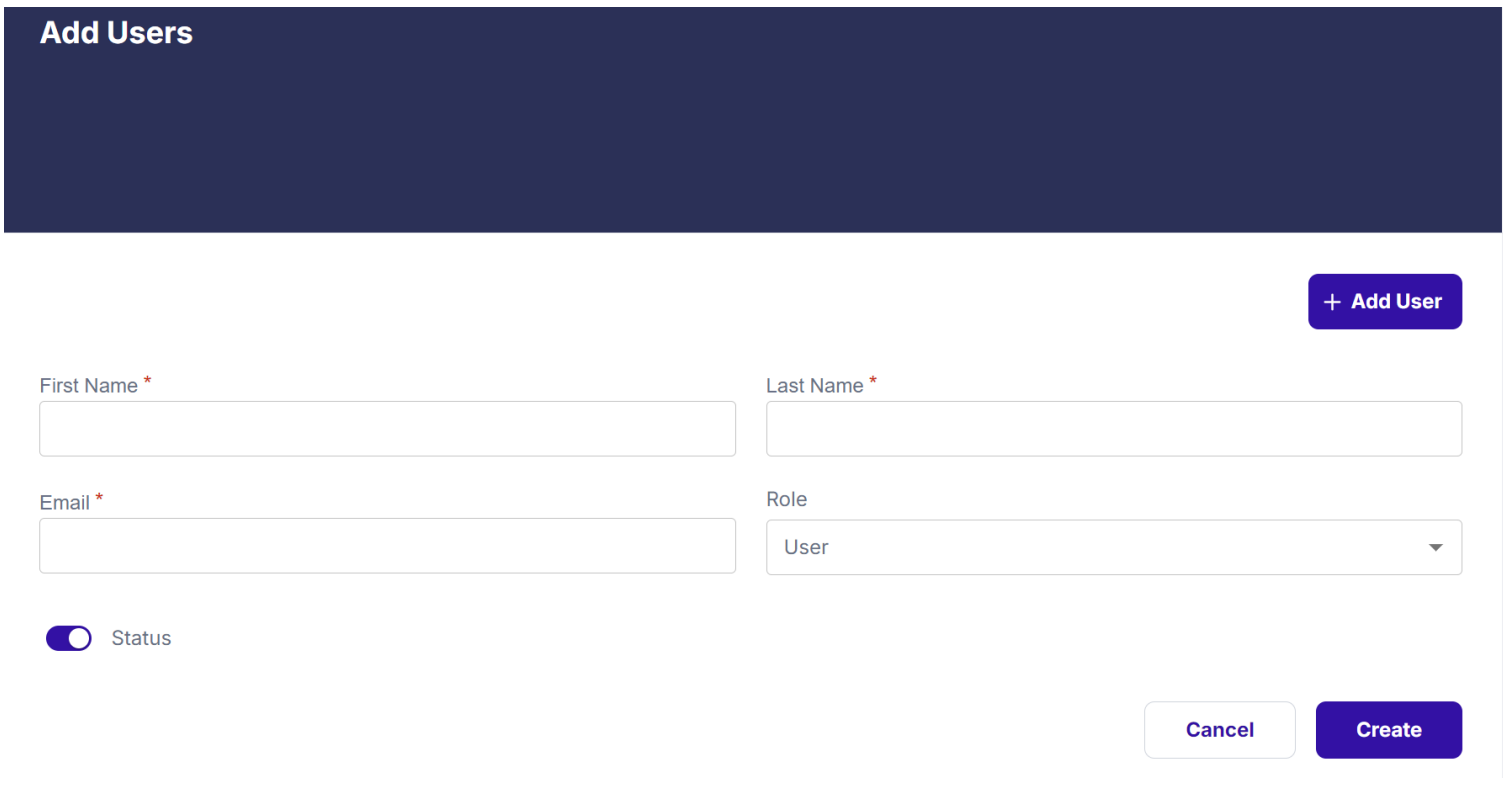


Figure 2: Adding a new user

3. Assign roles to the users. These roles determine what permissions and access levels the user will have in the system.

   There are two roles to pick from:

   - User: Access to specific test features like customised and standard tests but restricted from viewing sensitive areas like user management.
   - Admin: Can manage configurations (scenarios, merchants, devices) and has higher-level control than tenant users.#

> **Note:** For more information on what each role has access to, see Roles.

4. Click **Create** to finalise the user creation process.

You can view and edit details for a user from the User Management screen by clicking **See Details** for the user you want to edit.

> **Note:** Users cannot change their own email or roles. These settings can only be adjusted by an administrator.

Roles

The following table describes what each role has access to in the Payment Simulator Tool.

Modules	User	Admin
Customised Tests	Full Control	-
Standard Tests	Full Control	-
Scenarios	-	Full Control
Scenario Groups	-	Full Control
Cards with Value	Full Control	Full Control
Cards with Token	Full Control	Full Control
Merchants	-	Read Only
Acquirers	-	Read Only
Devices	-	Read Only
Acquiring Environments	-	Read Only
Connections	-	Full Control
Keys	-	Full Control
Users	-	Full Control
Decode Raw Message	Full Control	-
Compare Raw Message	Full Control	-

3 Configurations

The Configurations page enables you to test data for payment processing on the Payment Simulator Tool. These configurations are crucial for running both Customised and Standard tests.

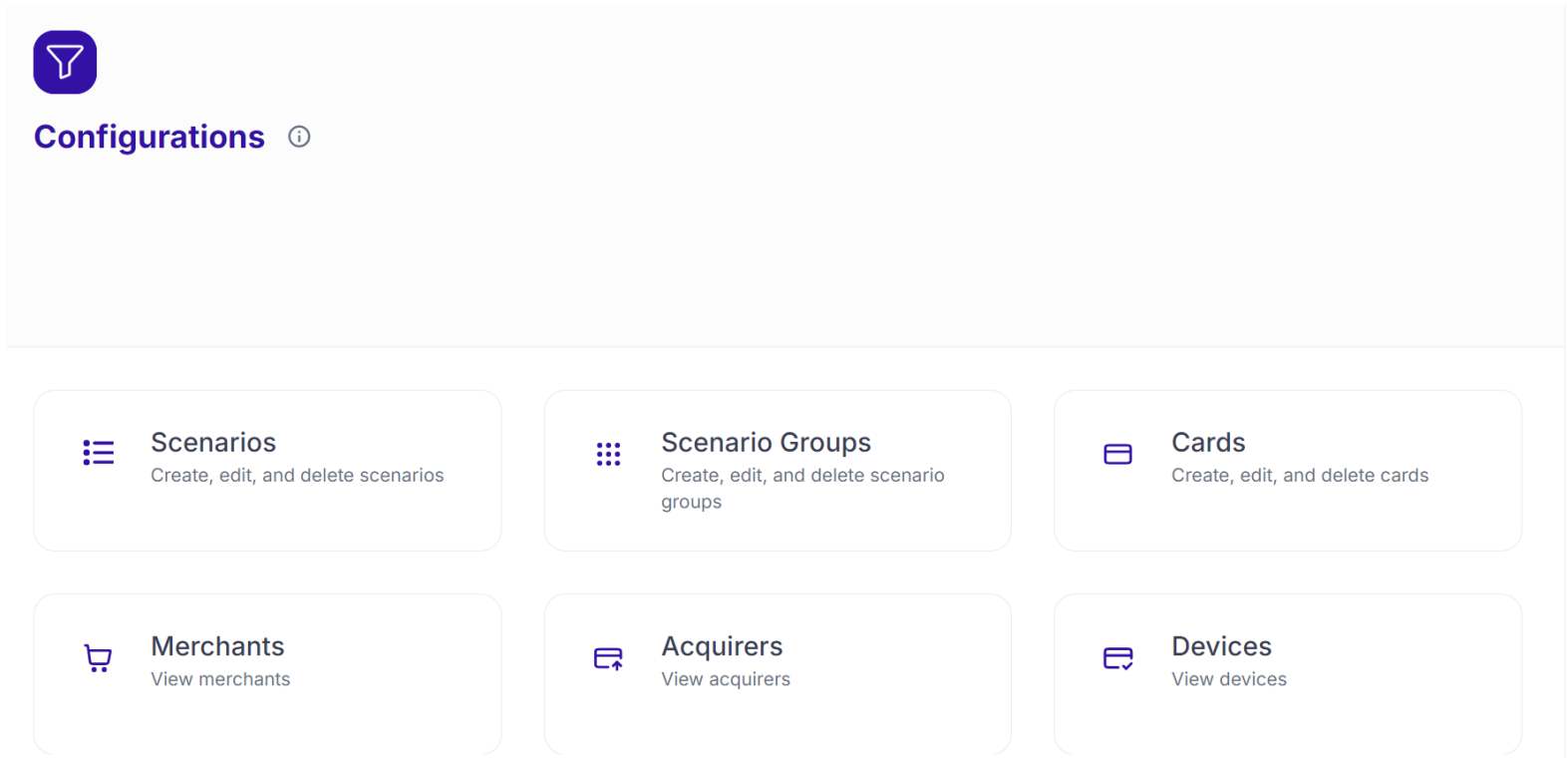


Figure 3: Configuration page - displaying test configuration options

The Configurations page consists of the following sections:

- **Scenarios:** Enables you to create, edit and delete test scenarios.
- **Scenario Groups**: Manage and group similar scenarios into a scenario group.
- **Cards:** Edit and manage different types of cards such as Visa, Mastercard and Discover.

  Note: You can only create cards using the Create Card API endpoint to create and maintain cards for use with the Payment Simulator Tool. When the card is created you can use the Cards section to manage the card. For more information, see the Cards API Documentation.
- **Merchants:** View the details of merchants who will be involved in your test transactions.
- **Acquirers:** View the entities responsible for processing payments on behalf of the merchants.
- **Devices:** View the devices used for payment processing.
- **Acquiring Environments:** View the environments where payment transactions are conducted.

  Note: Keys is not currently available to customers.

Scenarios

Test scenarios are used to simulate various transaction processes, such as authorisation, reversals, or completion advice. From the Scenarios page you can create test scenarios that are used on the Payment Simulator Tool.

- Click **Scenarios** to view a list of scenarios on the platform.

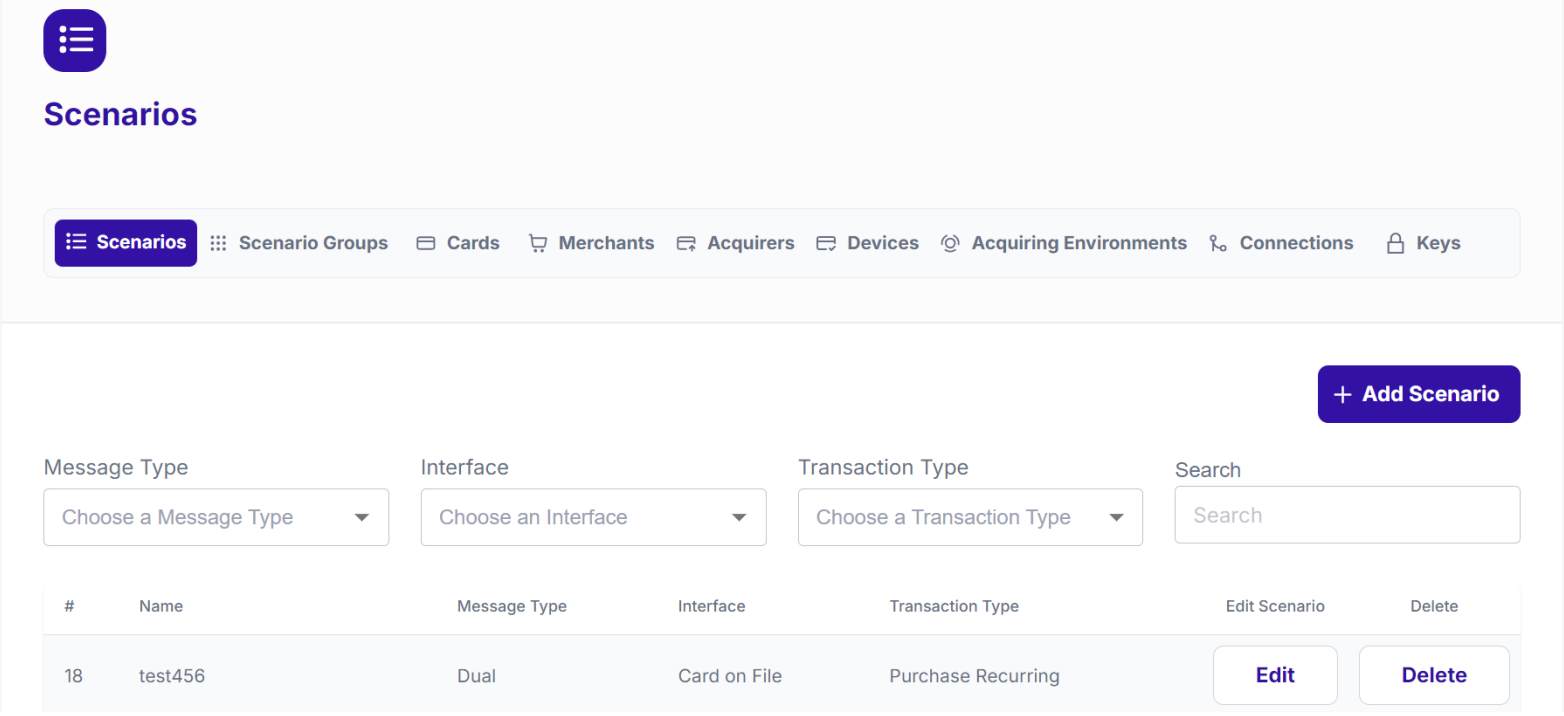


Figure 4: Scenarios page - listing current test scenarios

To create a scenario:

1. Click **Add Scenario**.
2. Enter the name of the scenario in the Scenario Name field. This should be a descriptive name that describes the nature of the scenario, such as Ecommerce Auth Test or STIP Advice Test.
3. Enter the test parameters for the first step of the scenario. For the first step, you should select available options such as Authorisation or STIP Advice. Select the appropriate Message Type and Interface Type and other required fields for the transaction.
4. Click **Add Step** to create a subsequent step. For subsequent steps, you can choose from Incremental Auth, Full Reversal, Partial Reversal, Completion Advice, or STIP Advice.

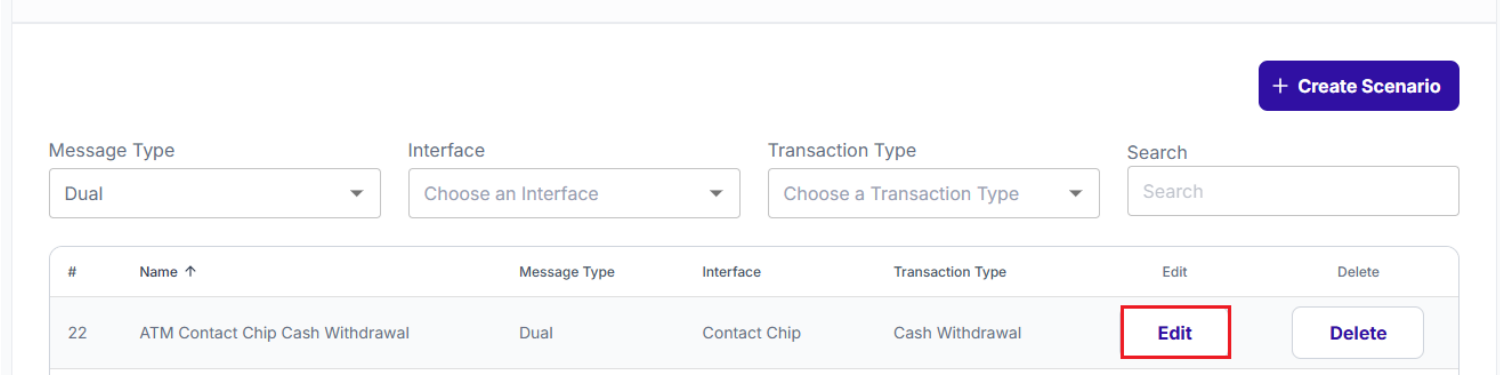
   The Message Type can be:

   - Dual, which processes transactions in two distinct steps (authorisation and settlement).
   - Single, which processes transactions in a single message.
   - Non-Financial, which are tests that do not directly involve monetary transactions but are essential for ensuring that systems function correctly.
   - Interface Type, which focuses on verifying the interactions between different software components, particularly where data exchange occurs. For example Card on File or Contact Chip.

   Note: For more information on the differences between dual and single message systems, see Dual vs. Single Message Systems.
5. Add **Expected Response Fields**. You need to add at least one field. You can create a custom field by specifying a field name and value, then click **Add**.
6. Enter an optional request in the Request Fields section. This allows you to enter any specific field values you want to include in the test request. When you click **Request Fields**, the template will update based on the interface type, transaction type, and selected card network. If you need a custom field not available in the template, you can manually add it by entering the field name and value, then clicking **Add**.
7. Click **Save** to save the scenario.

To edit an existing test scenario:

1. Click **Edit** for the scenario you want to edit.



2. Amend the details of the scenario as required. You can access the Expected Response Fields and Request Fields for each step of the test scenario, allowing you to adjust the fields as needed.
3. Click **Save**.

To delete a scenario, click **Delete** next to the scenario name.

Scenario Groups

Scenario groups allow users to bundle multiple test scenarios together and run them as a batch, making the testing process more efficient.

Note: You must create scenarios first before you can add them to a scenario group.

- Click **Scenario Groups** on the Configurations page to view a list of scenario groups on the platform.

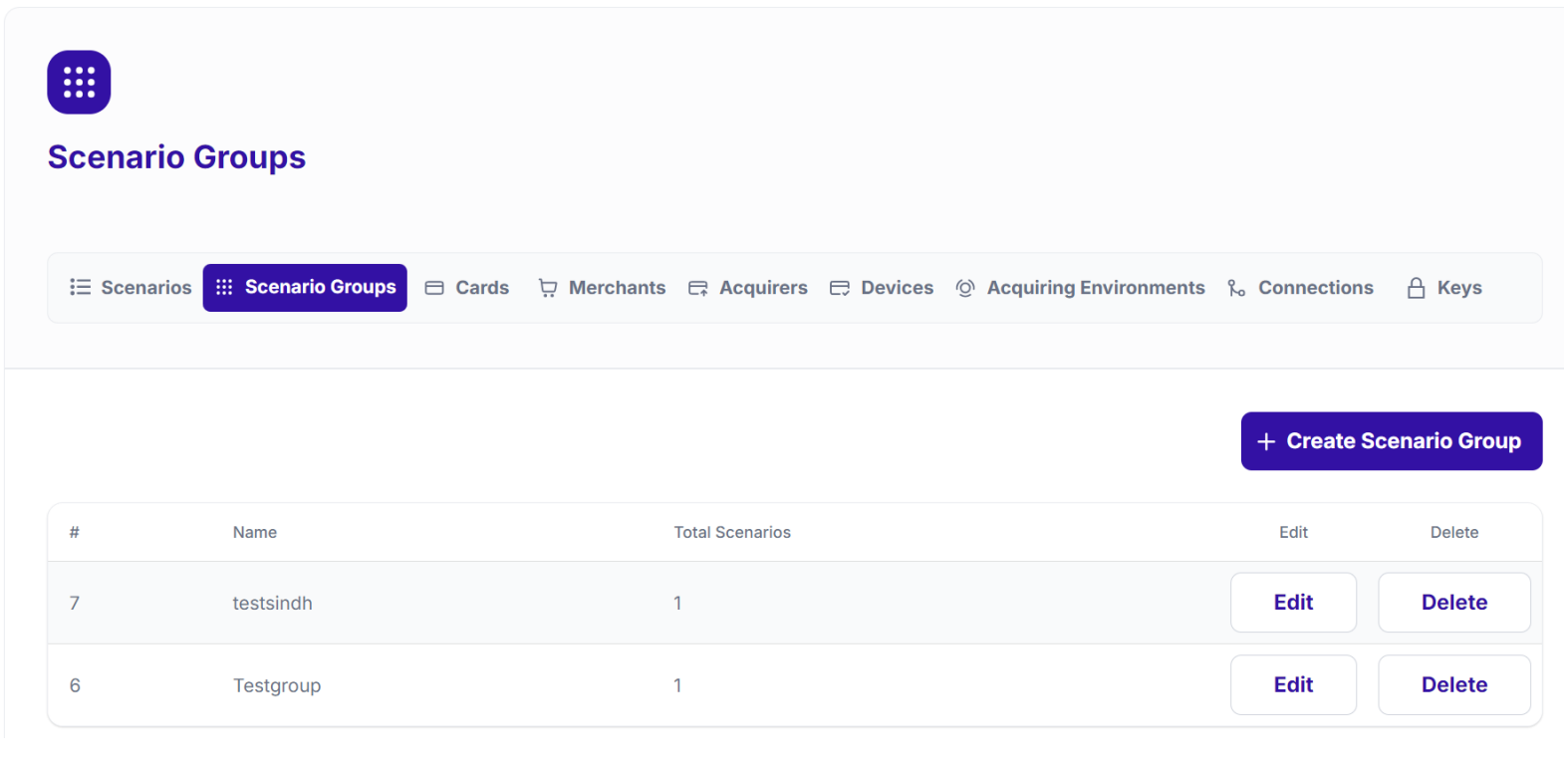


Figure 5: Scenario Groups page - for running test scenarios in batches

To create a scenario group:

1. Click **Create Scenario Group**.
2. Use the Filter option to narrow down the scenarios based on message type, interface, and transaction type. This helps you quickly locate the scenarios that you want to include in your group.
3. Enter a scenario group name in the **Scenario Group Name** field.
4. Select the **Scenarios to Include in the Group**. From the filtered list, select the individual scenarios that you want to add to the scenario group.
5. Click **Create** to save the scenario group.

To edit an existing scenario group:

1. Click **Edit** for the scenario group you want to edit.
2. Edit the details for the scenario group as required. This allows you to update the group's name, add or remove scenarios, or modify any scenario details.
3. Click **Save**.

To delete a scenario group, click **Delete** next to the scenario group name.

Cards

The Cards section enables you to add new cards to use in the Payment Simulator Tool. Cards can be created using the Create Card endpoint. For more information, see the Cards API Documentation.

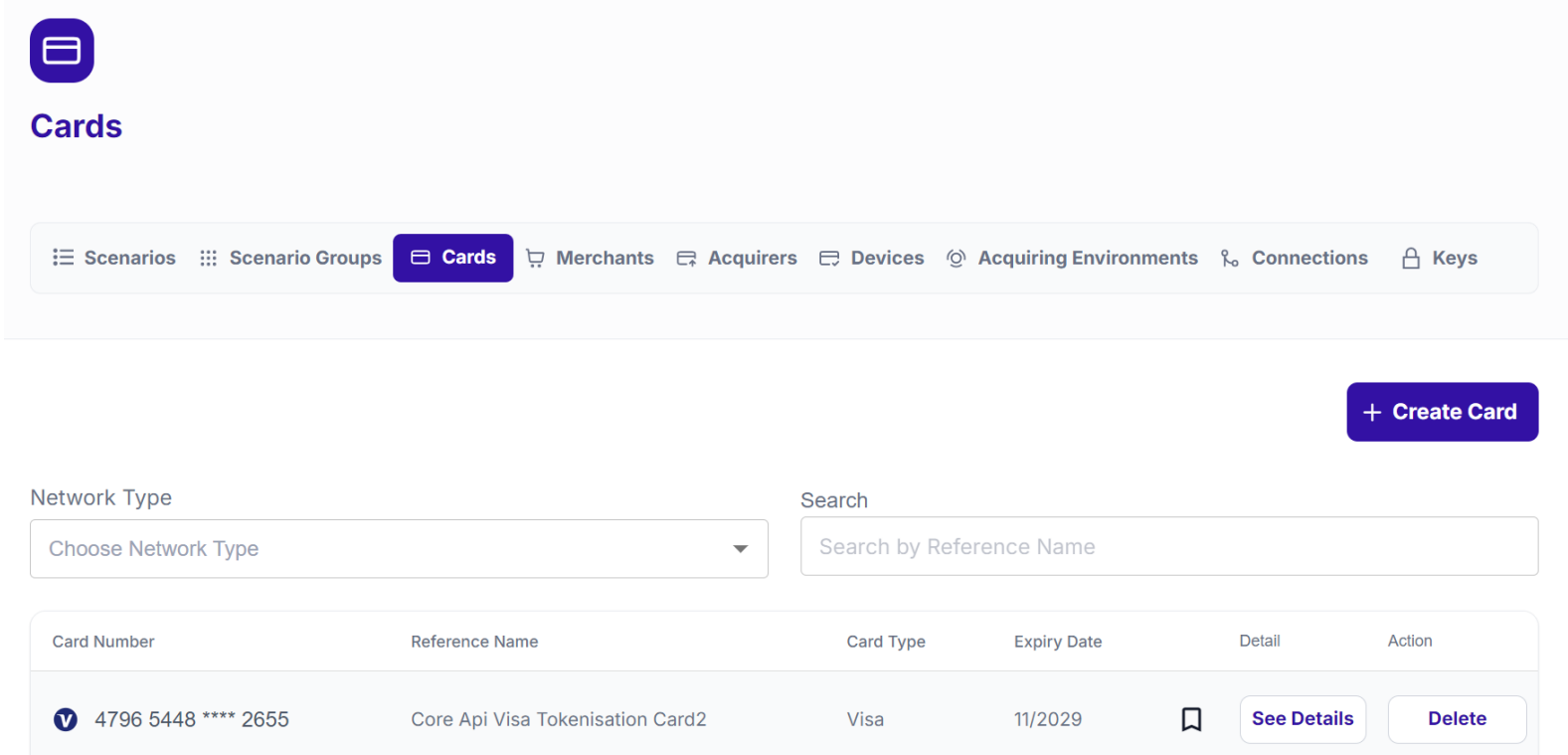


Figure 6: Cards page - enables adding cards for testing

To add a new card:

1. Click **Create Card**.
2. Enter the details for the card in the fields provided. Ensure that all required fields, marked with a red asterisk (*), are filled out before saving the record. Missing information in these fields may cause errors during the test execution.
3. Click **Create**.

To edit an existing card:

1. Click **See Details** for the card you want to edit.
2. Edit the details of the card using the fields provided.
3. Click **Save**.

To delete a card, click **Delete** next to the card you want to delete.

Connections

The Connections page enables you to configure network connections, so administrators can ensure proper set up for transaction routing. This is managed externally, so you do not need to manage or maintain connections. If the connection is down raise a customer support ticket.

Acquiring Environments (Merchants, Acquirers and Devices)

Note: Acquiring environments are for admin users only.

This section provides detailed instructions for viewing merchants, acquirers, and devices in the Payment Simulator Tool. You cannot create or edit merchants, acquirers or devices from their respective pages. You can only view the details for each existing environment.

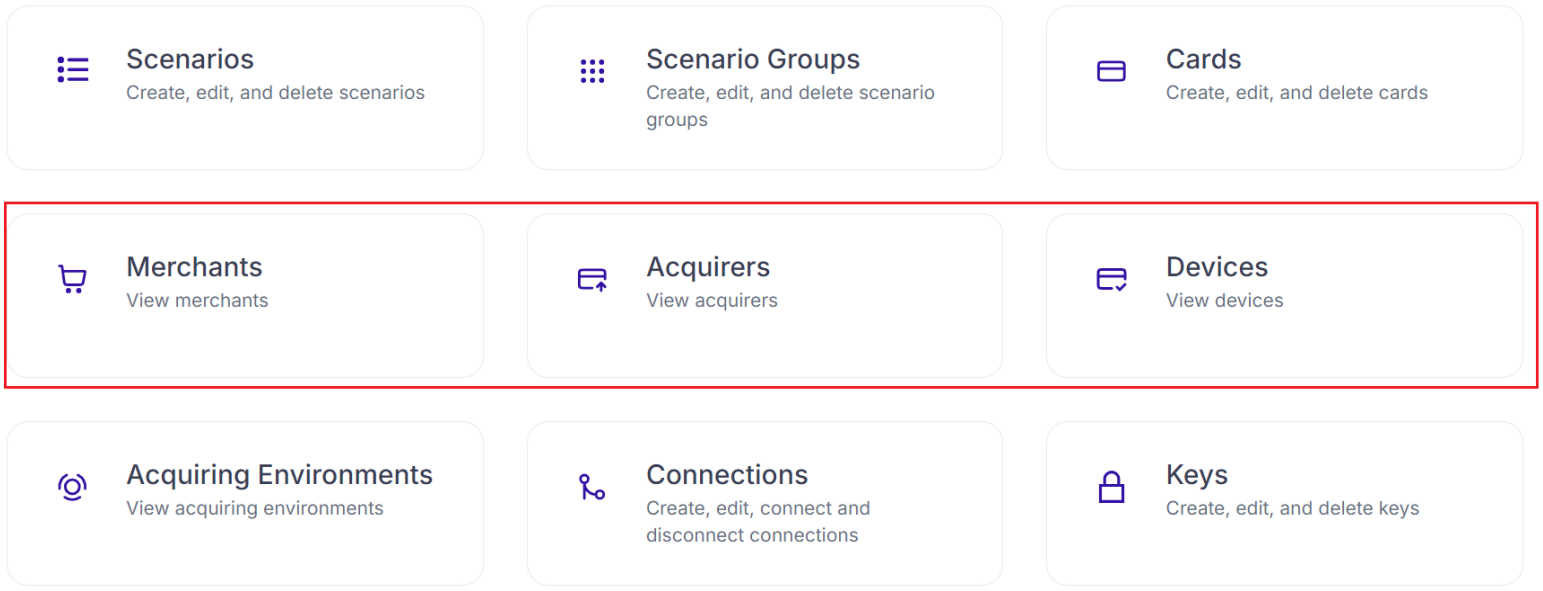


Figure 7: Managing acquirer, merchant details and devices details to be used during test scenarios

To view the details for a merchant:

1. Click **Merchants**. The Merchants page opens.
2. Click **See Details** for the merchant you want to view. The Merchant Details page opens, enabling you to view details for the merchant selected.

To view the details for an acquirer:

1. Click **Acquirers**. The Acquirers page opens.
2. Click **See Details** for the acquirer you want to view. The Acquirers Details page opens, enabling you to view details for the acquirer selected.

To view the details for a device:

1. Click **Devices**. The Devices page opens.
2. Click **See Details** for the device you want to view. The Device Details page opens, enabling you to view details for the device selected.

4 Customised Tests

The Customised Test screen for Payment Simulator Tool enables you to simulate the entire lifecycle of a card payment transaction. This customisation enables in-depth testing of various scenarios within your payment processing system.

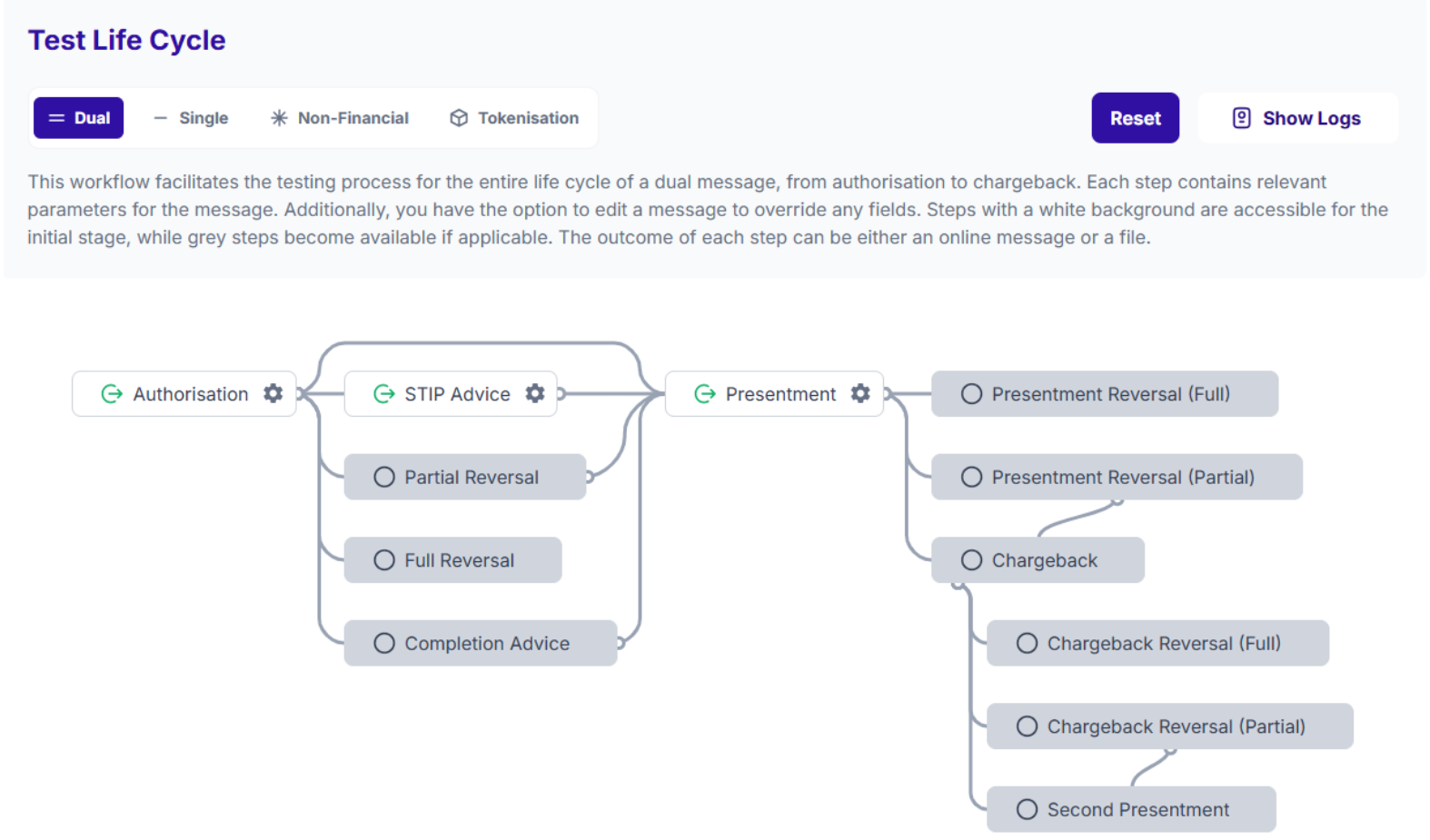


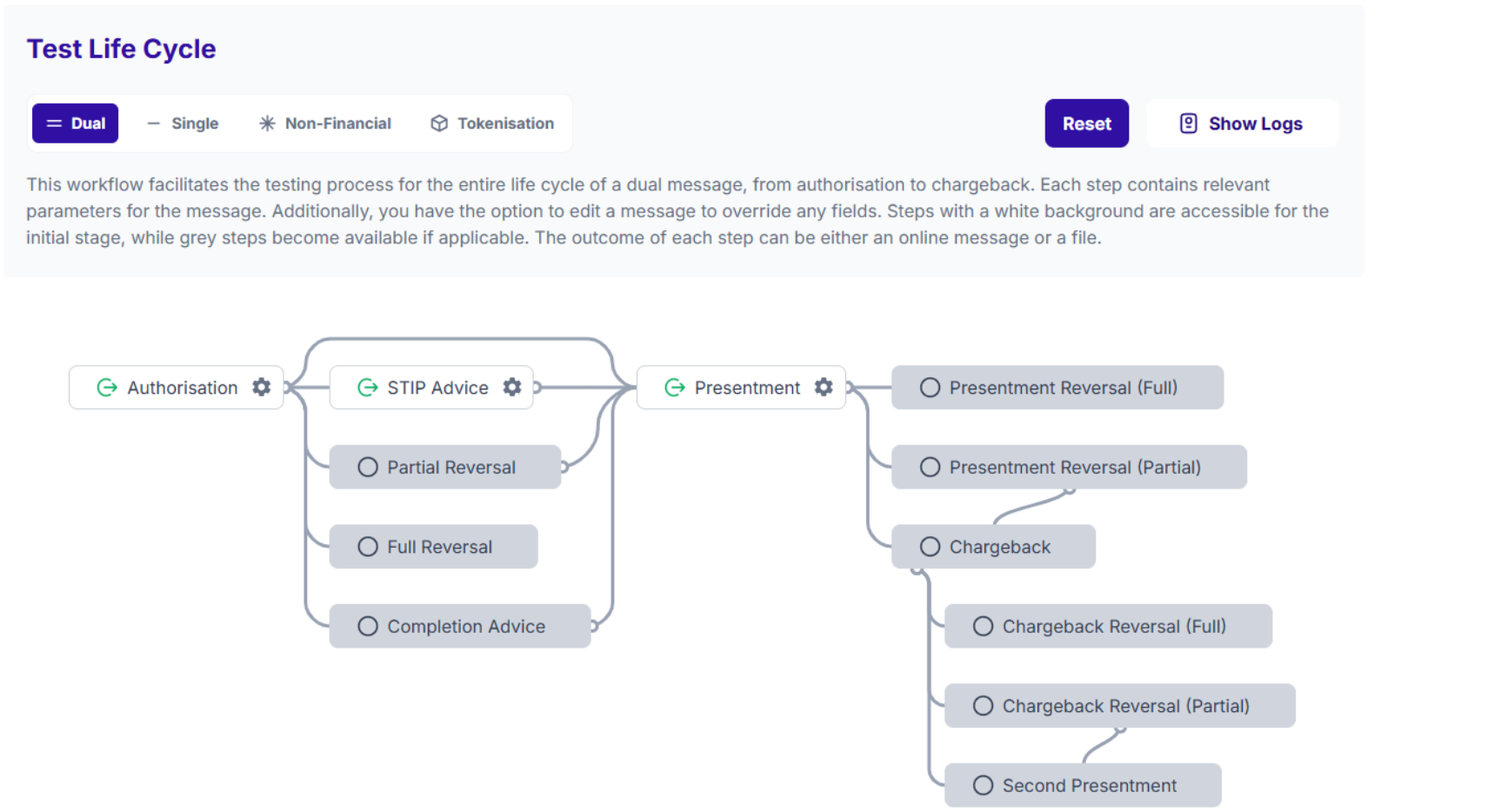
Figure 8: Customised Test Screen

The top of the Customised Tests page displays the available network connections, such as Visa, Mastercard and Discover.

- **Dual** – refers to the card having contact (EMV chip), contactless (NFC) or magstripe capabilities. A dual life-cycle means the card can support both chip-based transactions (using EMV technology for enhanced security) and magstripe transactions (which is the traditional way of swiping a card).
- **Single** – refers to the testing process for the entire life cycle of a single message, from financial message to chargeback.
- **Non-Financial** – means that the transaction type does not involve a financial movement (such as a payment or withdrawal), but is instead related to operations like validation, tokenisation, or updating credentials.
- **Tokenisation** – refers to the process of replacing the sensitive card data (PAN) with a token. Tokens are used to complete transactions without exposing the actual card number, making the transaction more secure. The token is mapped back to the original PAN by a trusted third-party (For example, Visa or Mastercard).

Test Life Cycle

The Test Life Cycle section allows you to simulate the complete transaction process. To perform a test of the transaction life cycle select a test type.



Select from one of:

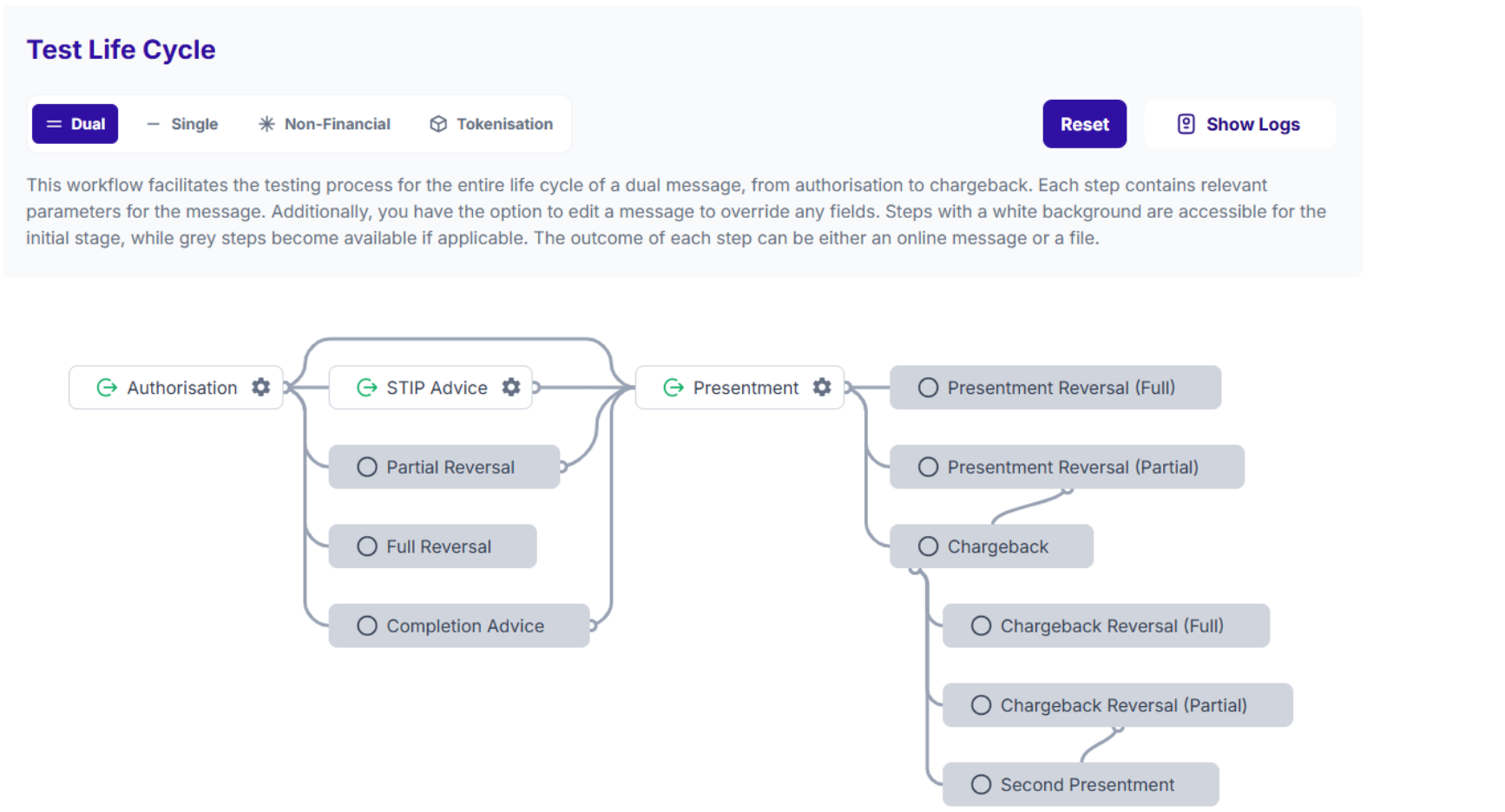
- Dual Message, where tests involve two message exchanges. For example, authorisation followed by clearing.
- Single Message, where tests require only one message to complete the transaction.
- Non-Financial, where tests simulate actions like balance inquiries or PIN changes that do not involve financial transactions.
- Tokenisation, where tests simulate the process of converting card information into a token for secure future use.

The different tests are detailed in the following sections.

Dual Message Test

This workflow facilitates the testing process for the entire life cycle of a dual message, from authorisation to chargeback. Each step contains relevant parameters for the message. Additionally, you have the option to edit a message to override any fields. Steps with a white background are accessible for the initial stage, while grey steps become available if applicable. The outcome of each step can be either an online message or a file.

Note: Parameters for the message can only be added by a system admin.



The Dual Message test consists of the following steps:

- Authorisation: The first step where the transaction is initially approved or denied based on the cardholder's details and account status.
- STIP Advice: Optional step used for sending supplemental transaction information
- Settlement: Conducts preliminary settlement processing
- Settlement Reversal (Full and Partial): Reverses a previously processed settlement either fully or partially.
- Chargeback and Chargeback Reversal (Full and Partial): Manages disputes related to transactions and reverses chargebacks as necessary.
- Completion Advice: Finalises the transaction with a completion message.
- Second Settlement: Handles scenarios requiring a second settlement process

For each step, you will be able to input specific parameters such as Interface, Message Type, Transaction Type, Merchant, and Card Details. All fields in a message are editable, allowing you to tailor the test to meet specific conditions or requirements.

Note: For more information on the differences between dual and single message systems, see Dual vs. Single Message Systems.

Perform a Dual Message Test

To perform a dual message test:

1. Select **Dual Message**.
2. Click **Authorisation** to check the transaction's validity.
3. Enter the parameters for the authorisation using the fields provided. The fields change depending on the Transaction Type and interface selected.

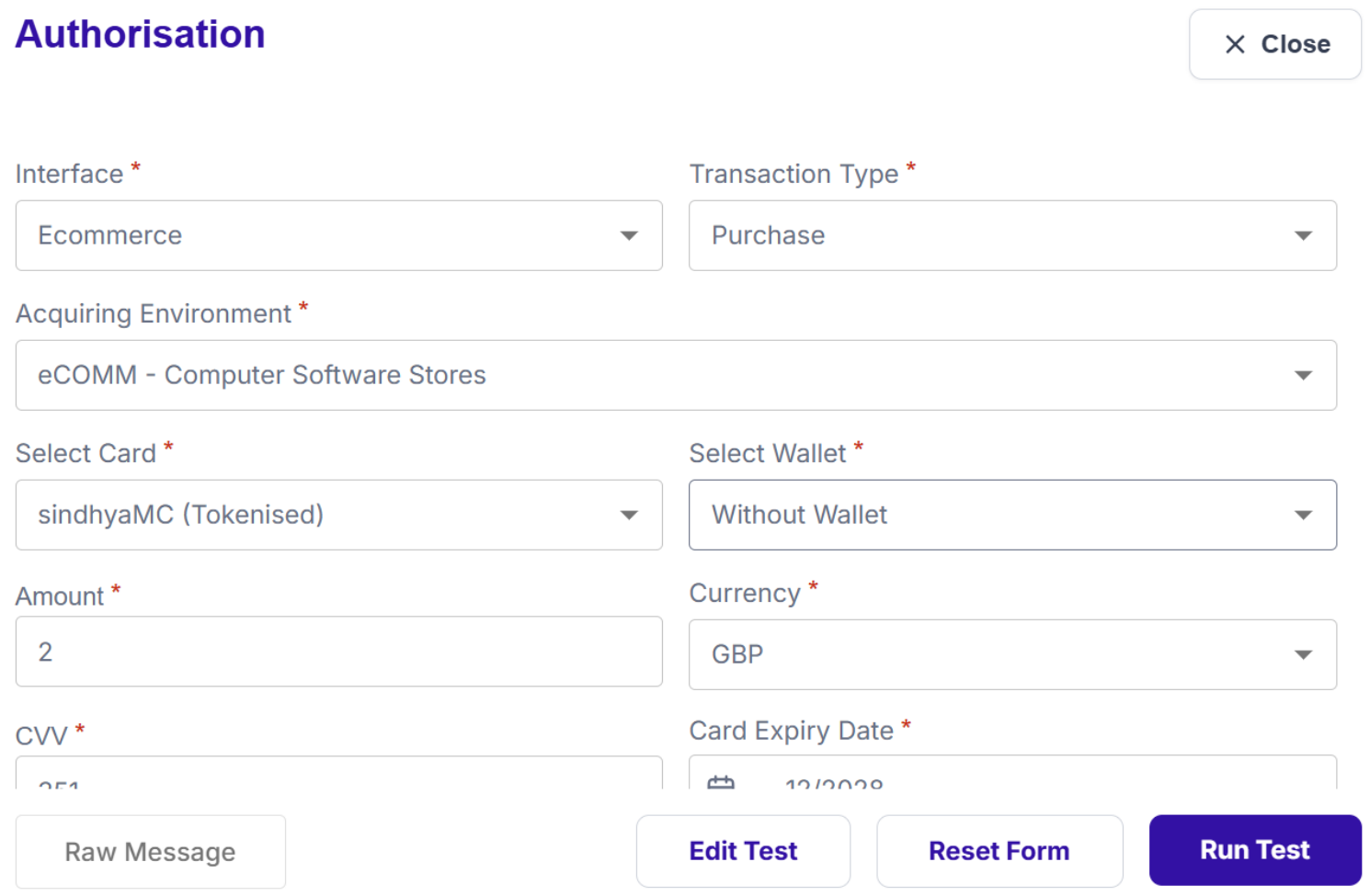


Figure 9: Running a Dual Message authorisation test

4. Click **Run Test**.
5. (Optional) Click **STIP Advice** if additional information needs to be communicated during the transaction. The STIP Advice window displays where you can enter the amount of the STIP Advice, the Reason Code, and whether the STIP is accepted. Click Run Test to complete this stage of the test.

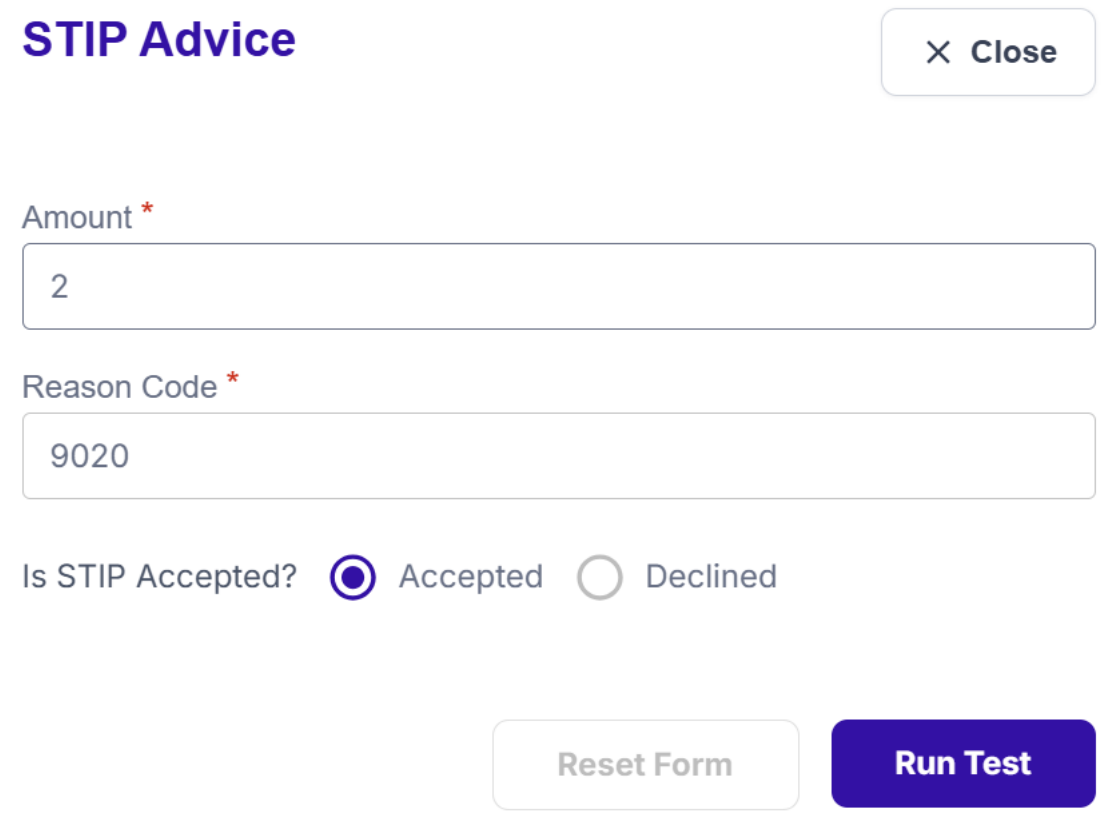


Figure 10: Running a Dual Message authorisation test - with STIP

Alternatively, select one of Partial Reversal, Full Reversal or Completion Advice as an optional phase before presentment.

6. Click **Presentment** to prepare the transaction for early settlement phases. The Presentment window displays with the value of the authorisation in the **Amount** field.
7. Click **Run Test** to complete this stage of the test.

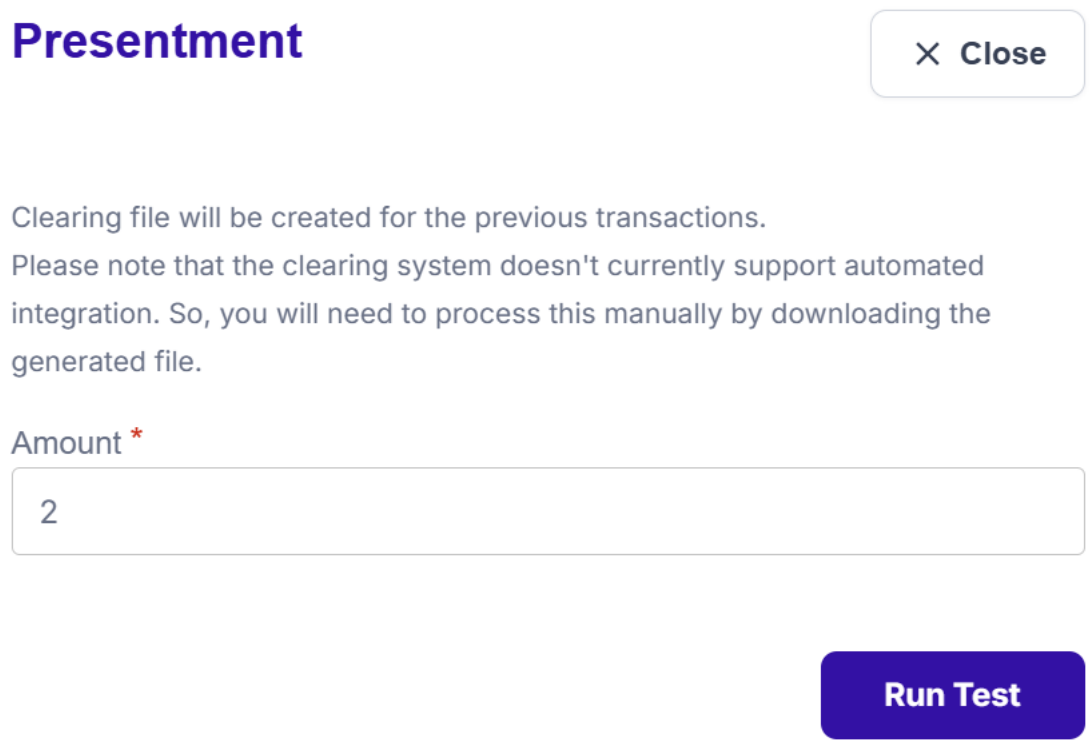


Figure 11: Run test with the presentment

8. Manage reversals and chargebacks. Utilise the relevant steps to handle transaction chargebacks or reversals.

Single Message Test

Note: Single Message is only applicable to US customers, or countries that implement Single Message System.

This workflow streamlines the testing process for the entire life cycle of a single message, from financial message to chargeback. Each step contains relevant parameters for the message. Additionally, you have the option to edit a message to override any fields. Grey steps become available if applicable.

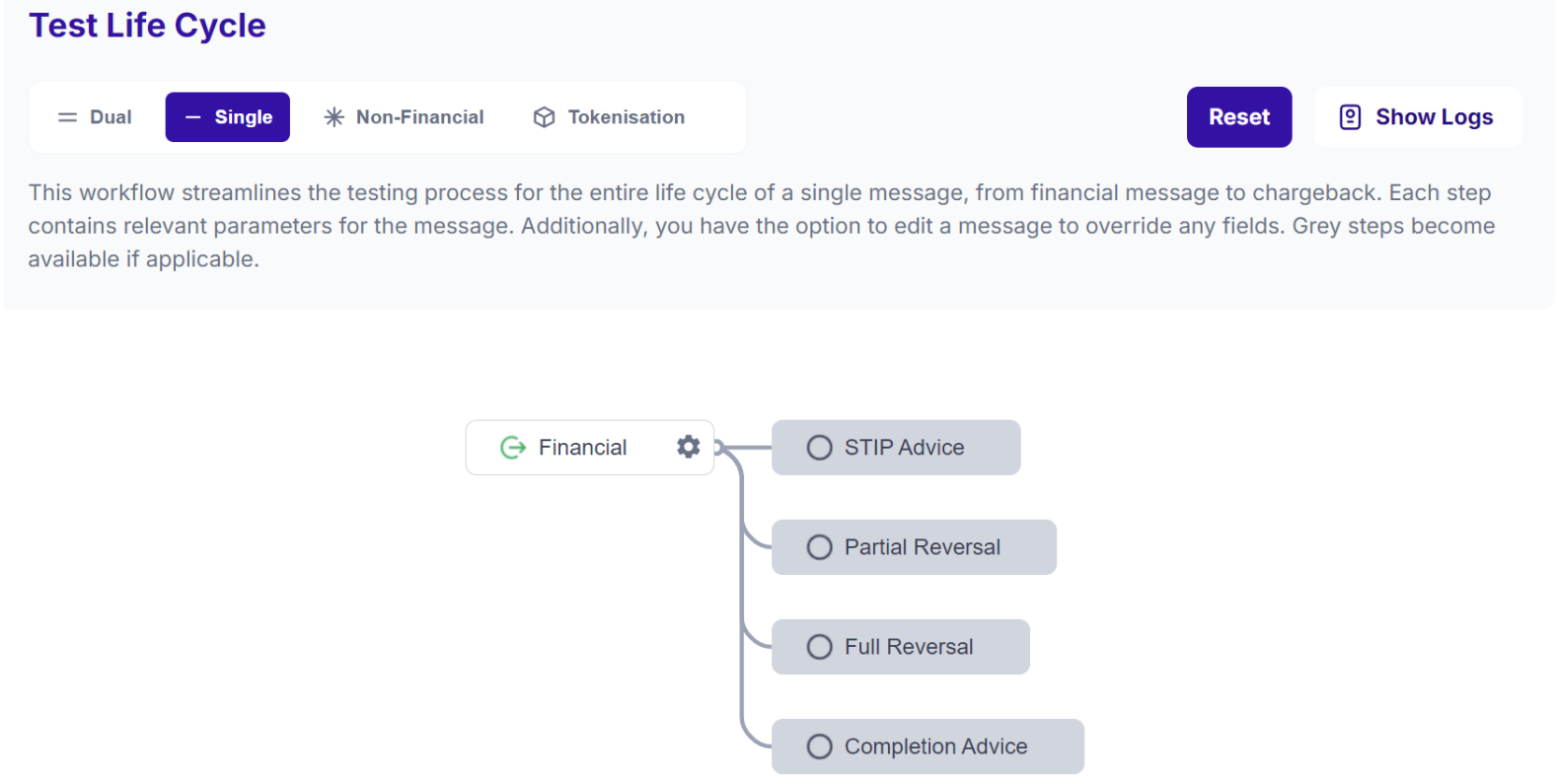


Figure 12: Test lifecycle in Single Message scenarios

Note: For more information on the differences between dual and single message systems, see Dual vs. Single Message Systems.

The Single Message test consists of the following steps:

- Financial: Initiate a single-message financial transaction.
- STIP Advice: Send or receive supplementary transaction information.

- Reversals (Partial and Full): Process transaction reversals as needed.
- Completion Advice: Finalise the transaction.

Perform a Single Message Test

To perform a Single Message test:

1. Click **Single** on the Test Life Cycle.
2. Click **Financial**.
3. Enter the parameters for the authorisation using the fields provided. The fields change depending on the Transaction Type selected.

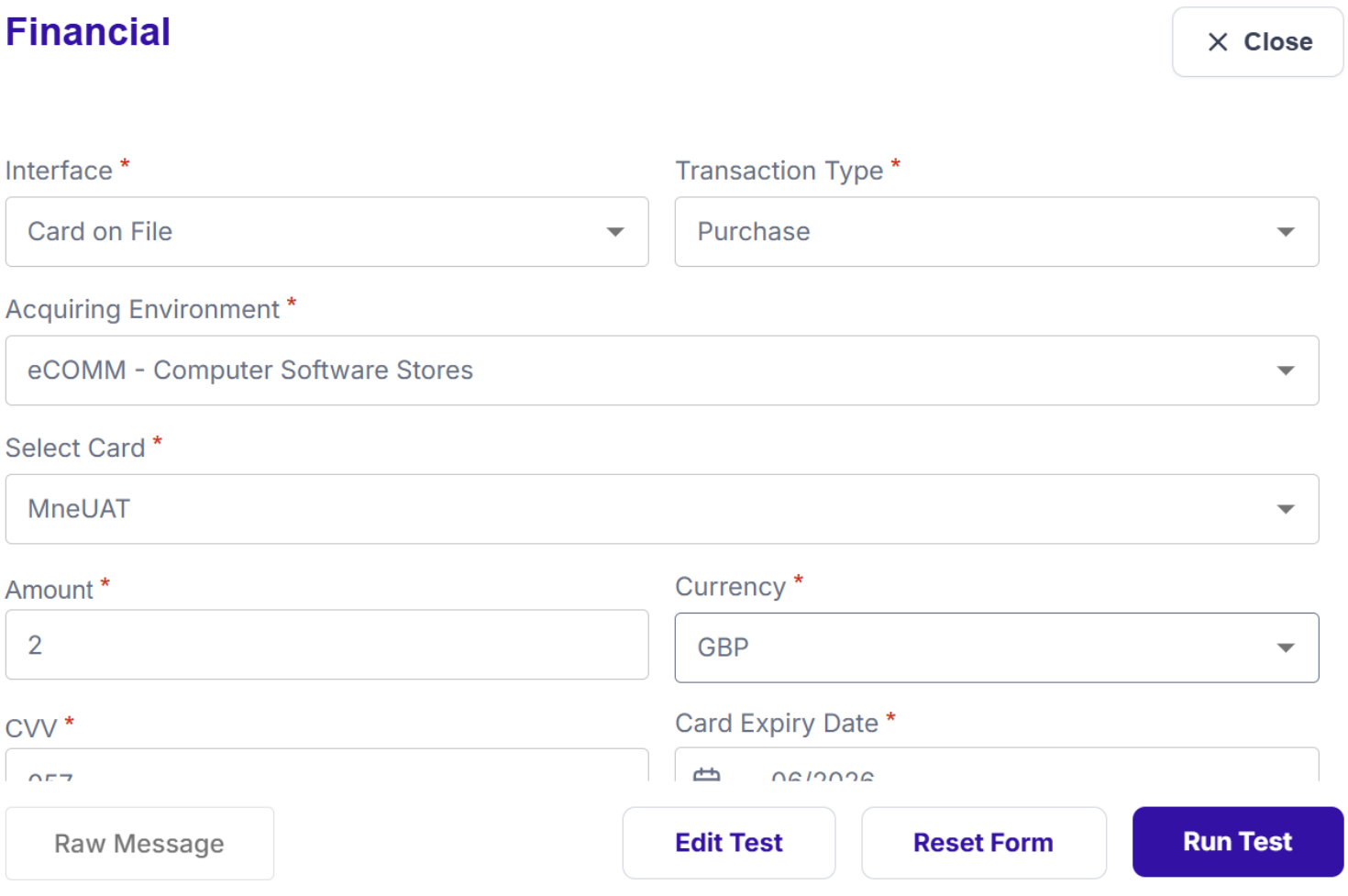
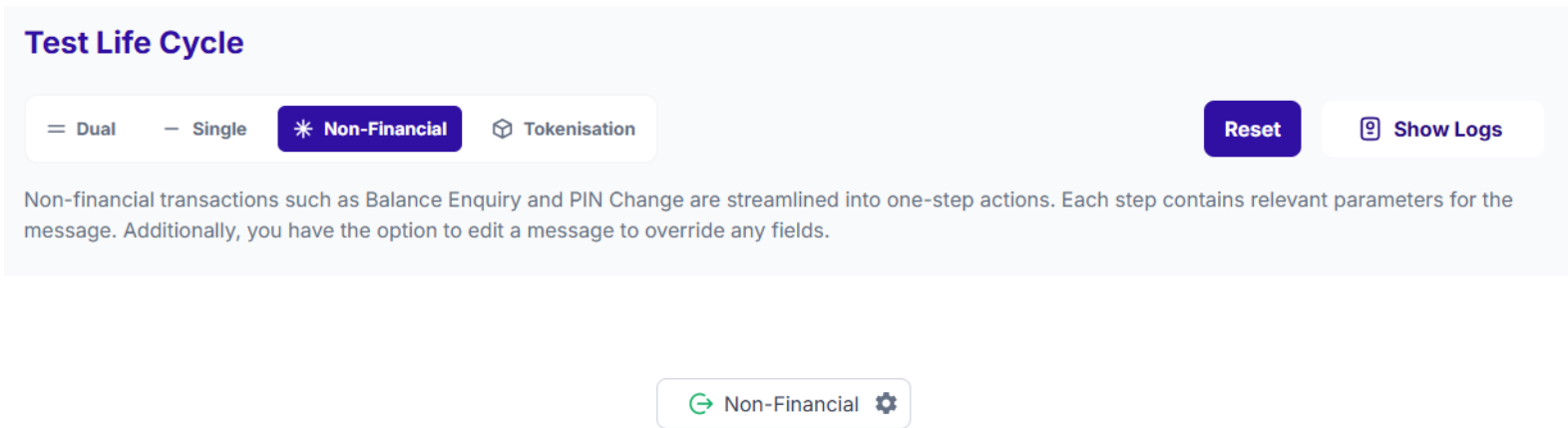


Figure 13: Running a Single Message test - financial message

4. Click **Run Test**.
5. (Optional) Click **STIP Advice** if additional information needs to be communicated during the transaction. The STIP Advice window displays where you can enter the amount of the STIP Advice, the Reason Code, and whether the STIP is accepted. Click Run Test to complete this stage of the test.
   Alternatively, select one of Partial Reversal, Full Reversal or Completion Advice as an optional phase.
6. Run the **Completion Advice** test to finalise the transaction.

Non-Financial Test

Non-financial transactions such as Balance Enquiry and PIN Change are streamlined into one-step actions. Each step contains relevant parameters for the message. Additionally, you have the option to edit a message to override any fields.



Perform a Non-Financial Test

The Non-Financial test is used for executing non-monetary transactions like updating or querying account information.

To complete a Non-Financial test:

1. Select **Non-Financial** on the Test Life Cycle.
2. Click **Non-Financial**.
3. Enter the parameters for the non-financial test using the fields provided. The fields change depending on the Transaction Type selected.

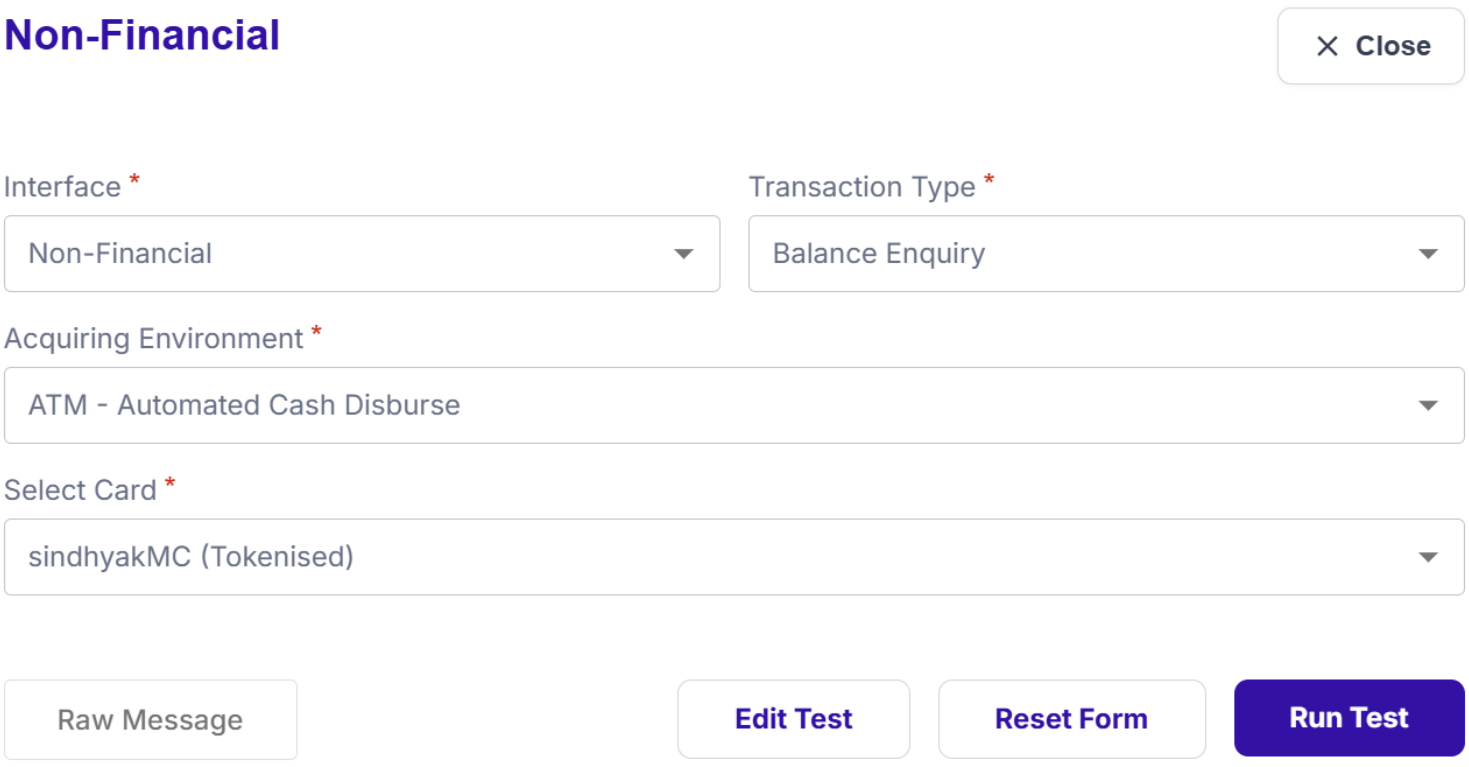
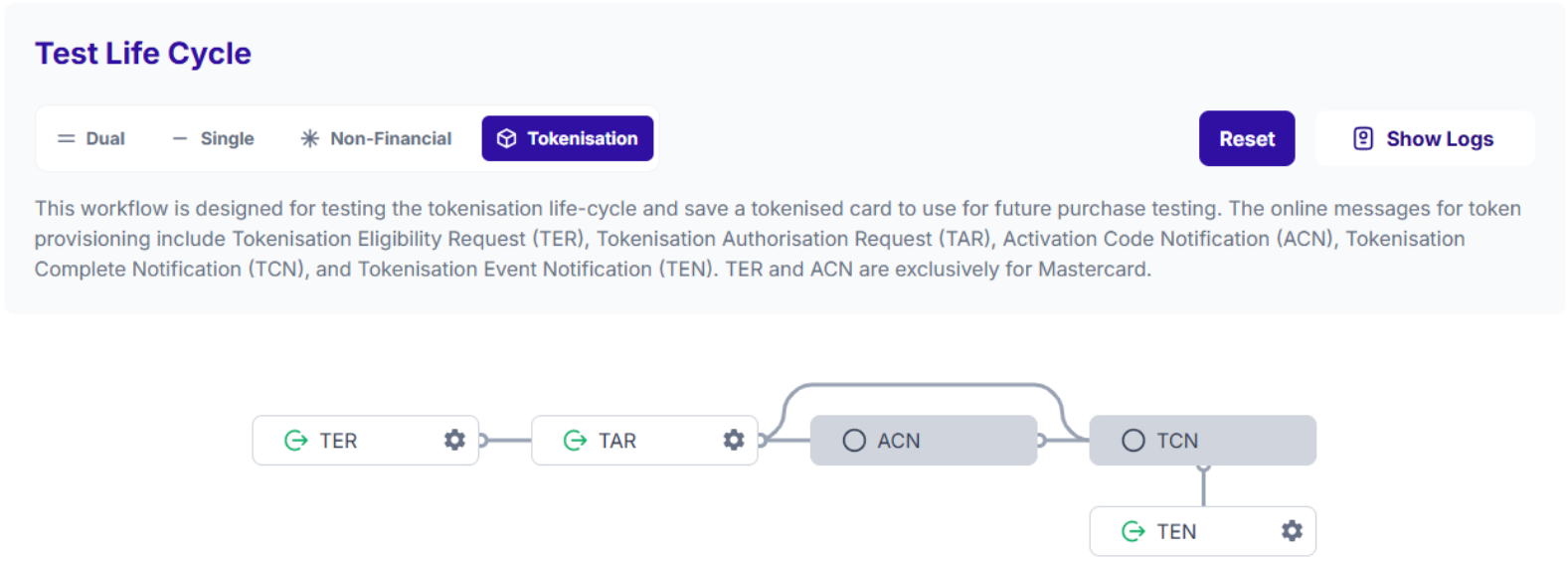


Figure 14: Running a Single Message test - non-financial message

4. Click **Run Test** .

Tokenisation Test

This workflow is designed for testing the tokenisation life-cycle. The online messages for token provisioning include Tokenisation Eligibility Request (TER), Tokenisation Authorisation Request (TAR), Activation Code Notification (ACN), Tokenisation Complete Notification (TCN), and Tokenisation Event Notification (TEN). TER and ACN are exclusively for Mastercard.



Note: For more information on Tokenisation, see the Tokenisation Service Guide.

Perform a Tokenisation Test

To complete a Tokenisation test.

1. Select **Tokenisation** on the Test Life Cycle.
2. Click **TER**.
3. Enter the details of the token using the fields provided. Select one of the following technologies to test:
    - Apple Pay
    - Google Pay
    - Samsung Pay
    - Merchant Tokenisation Program

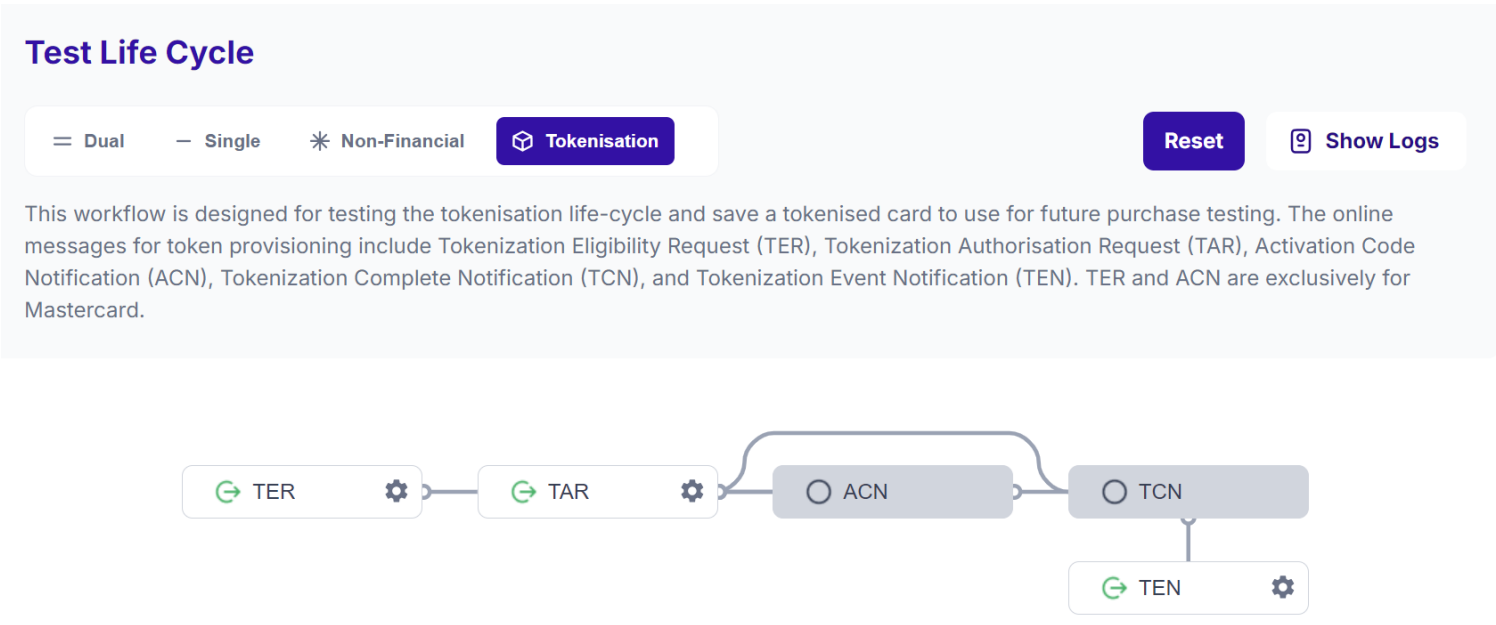


Figure 15: Tokenisation test workflow

4. Click **Run Test**.
5. Click **TAR**.
6. Enter the details, such as the Wallet Name and Wallet Reason Code. The default Device Score and Account Score values are set to 5, but you can modify them for testing purposes.To save the selected wallet, check the Enable Card for Tokenised Purchase check box. The wallet will only be saved when the TCN step succeeds.

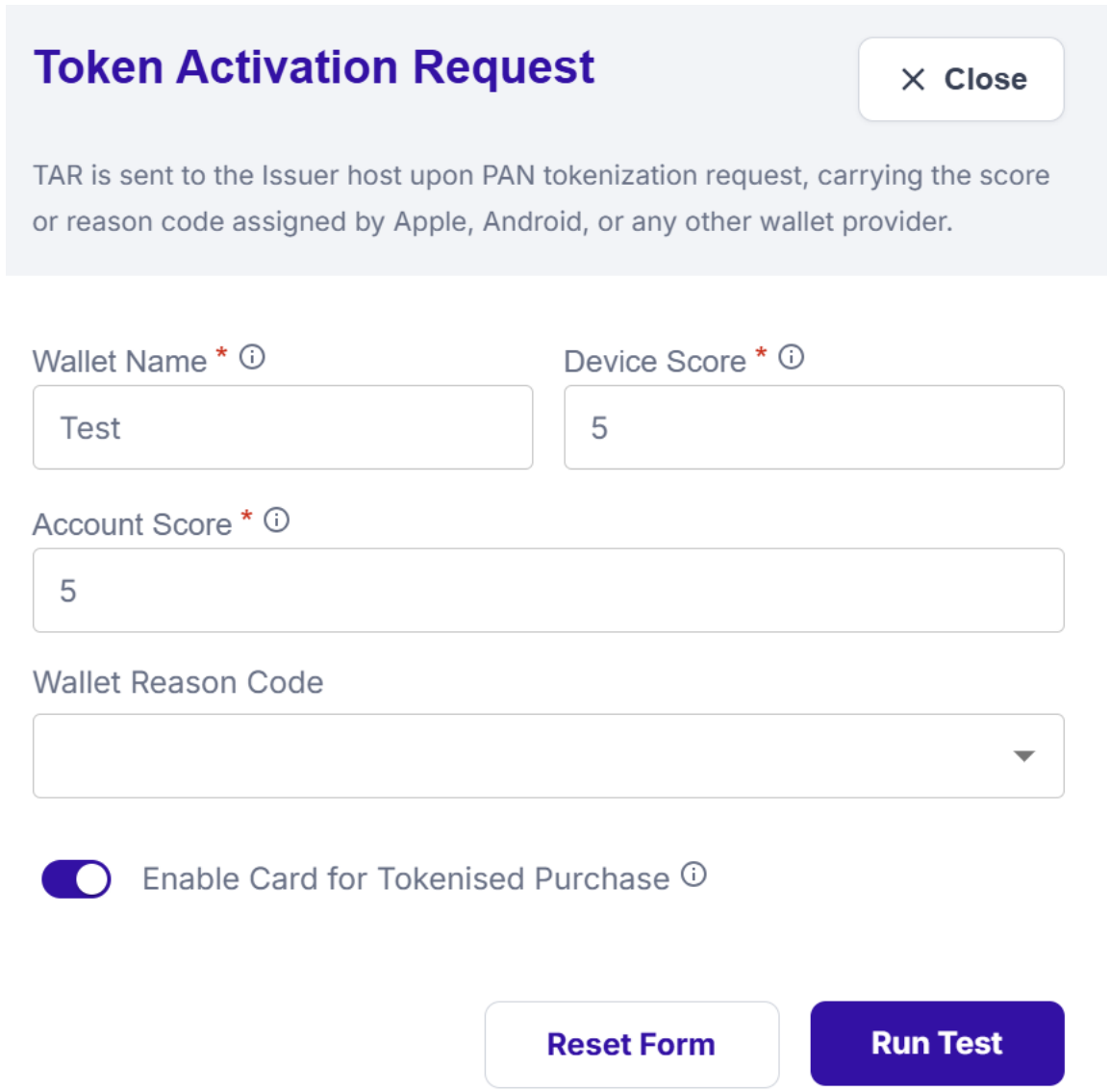


Figure 16: Running a Tokenisation test - Token Activation Request (TAR)

7. Click **Run Test**.
8. (Optional) Click **ACN**. This is enables you to send a network message specific to digitization services. It includes the Activation Code and Expiration Date/Time to be sent to the cardholder through their chosen communication channel.

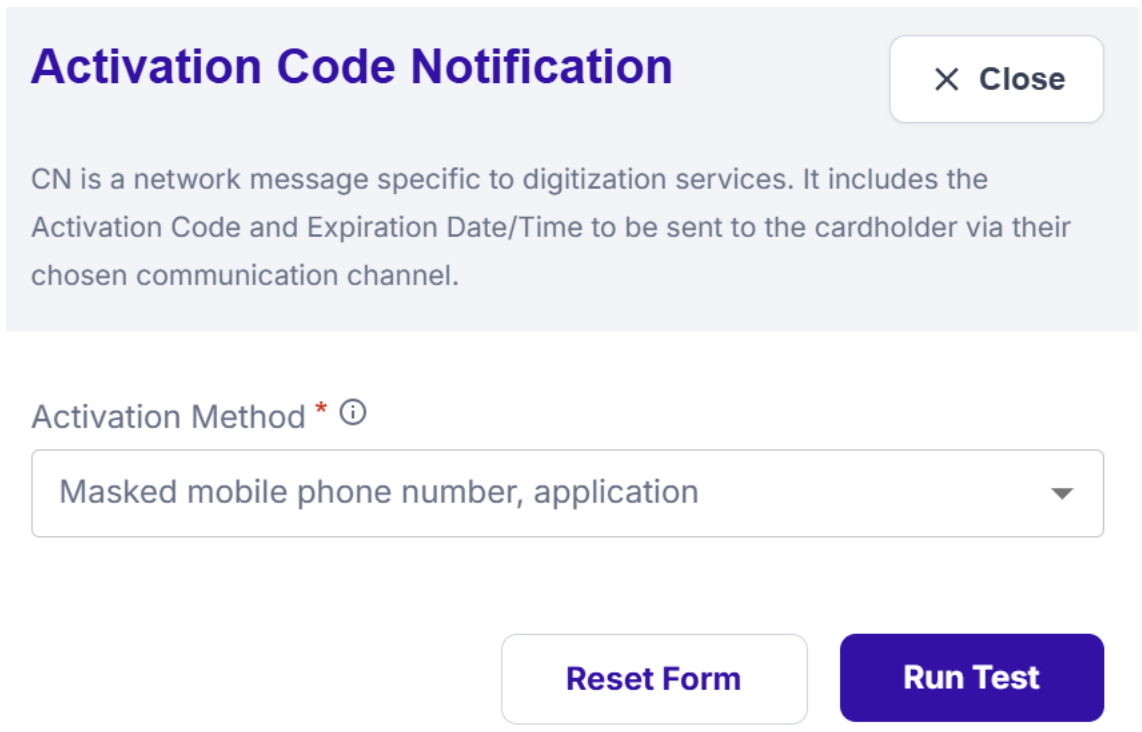


Figure 17: Running a Tokenisation test - Activation Code Notification (ACN)

9. Click **Run Test**.
10. Click **TCN**. When tokenization is finished, the Token Completion Notification (TCN) is sent by the payment network. This message provides details about the assigned token and other pertinent information related to the digitisation process.

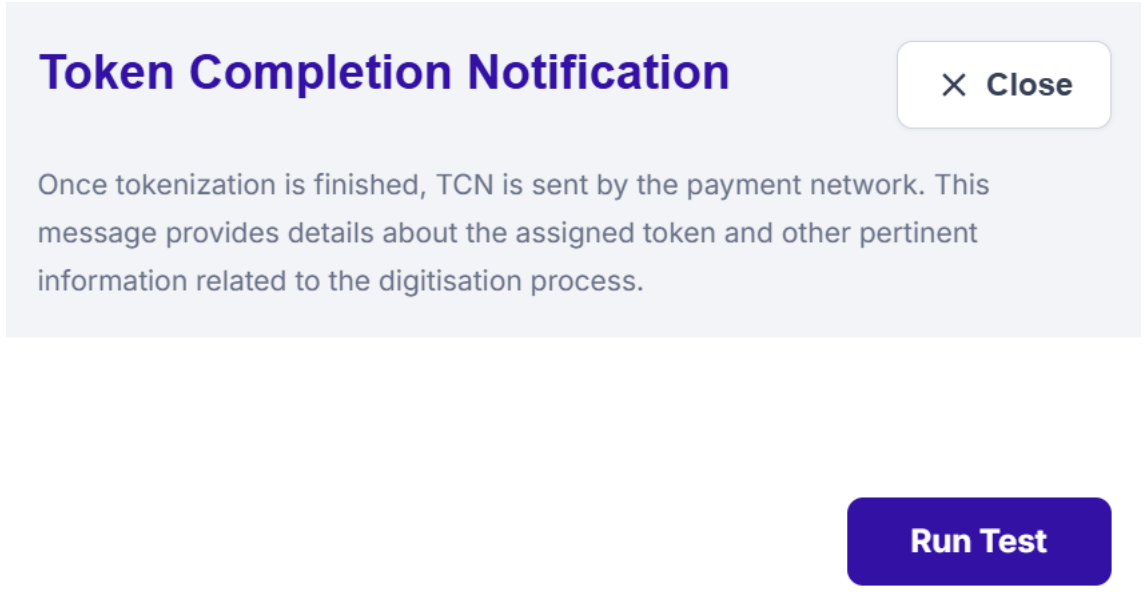


Figure 18: Running a Tokenisation test - Token Completion Notification (TCN)

11. Click **Run Test**.
12. Click **TEN**.
13. Select your wallet and an Event Indicator Code from the fields provided.

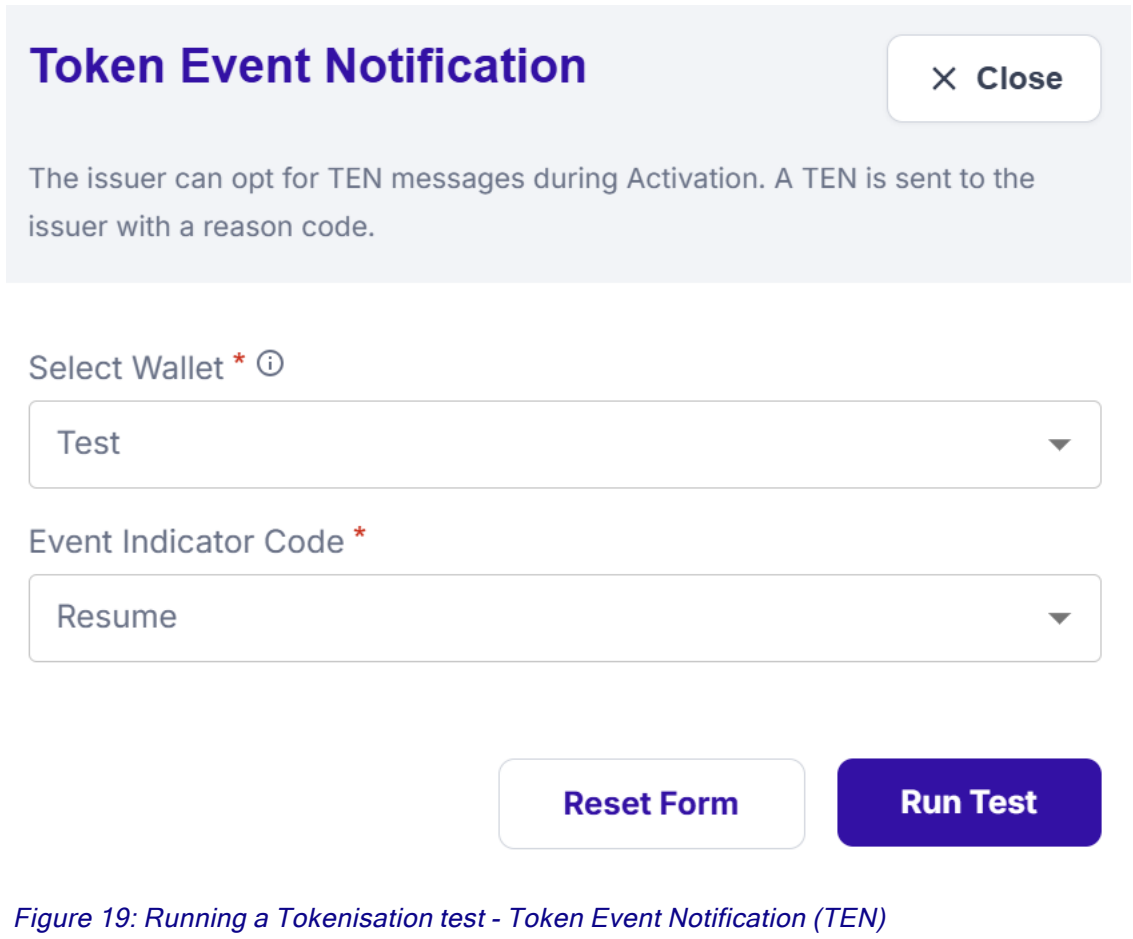


Figure 19: Running a Tokenisation test - Token Event Notification (TEN)

14. Click **Run Test**.

Note: For more information on each of these messages, see the Tokenisation Guide.

Test History

The Test History section is at the bottom of the Customised Tests and Standard Tests pages. This section lists all recent tests, with the most recent appearing first. From here, you can review logs, transaction data, and results from previously run tests, as well as resume any paused or incomplete tests. You can also continue a test that hasn't finished by clicking Resume.

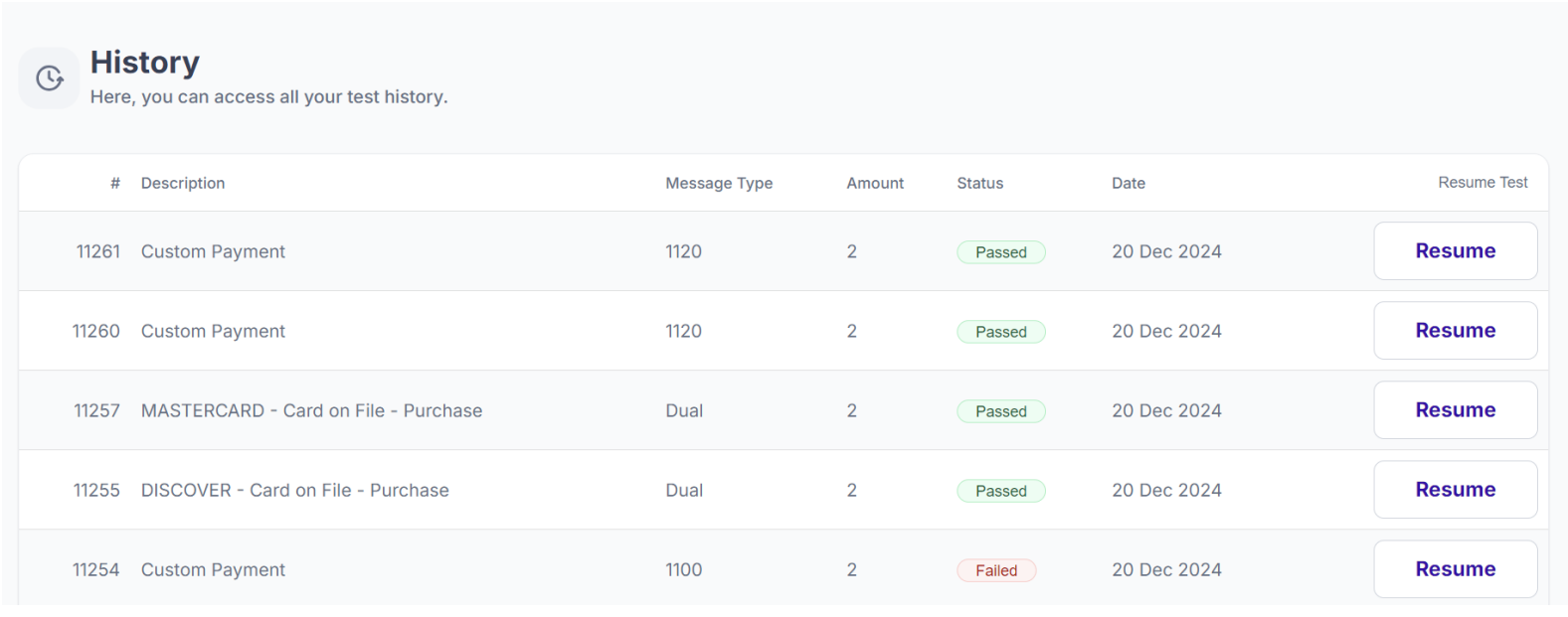


Figure 20: Viewing test history

Use Standard Tests

The Standard Test Page are pre-defined test cases for assessing the reliability of your payment systems across different scenarios. You can add or edit defined tests under **Configuration > Scenarios** or **Scenario Groups**.

This page offers a series of test cases related to card transactions that cover a broad range of scenarios.

Scenario Groups are tests that include different card types and transaction scenarios. Each test is associated with a specific card type (e.g., ATM, POS, online shopping). For each test, a specific card number to be tested can be selected. This is crucial for understanding how the tests work with various card types and technologies (For example, contact chip, contactless, magnetic stripe). Details like the status ("Not Run"), run time, and selected card information are displayed for each test case. Additionally, the outcome of each transaction can also be viewed.

Run a Standard Test

Note: You must create a test scenario before running a test. See Scenario Groups for more information.

To run a standard test:

1. Select a scenario group you want to test from the **Scenario Group** field.

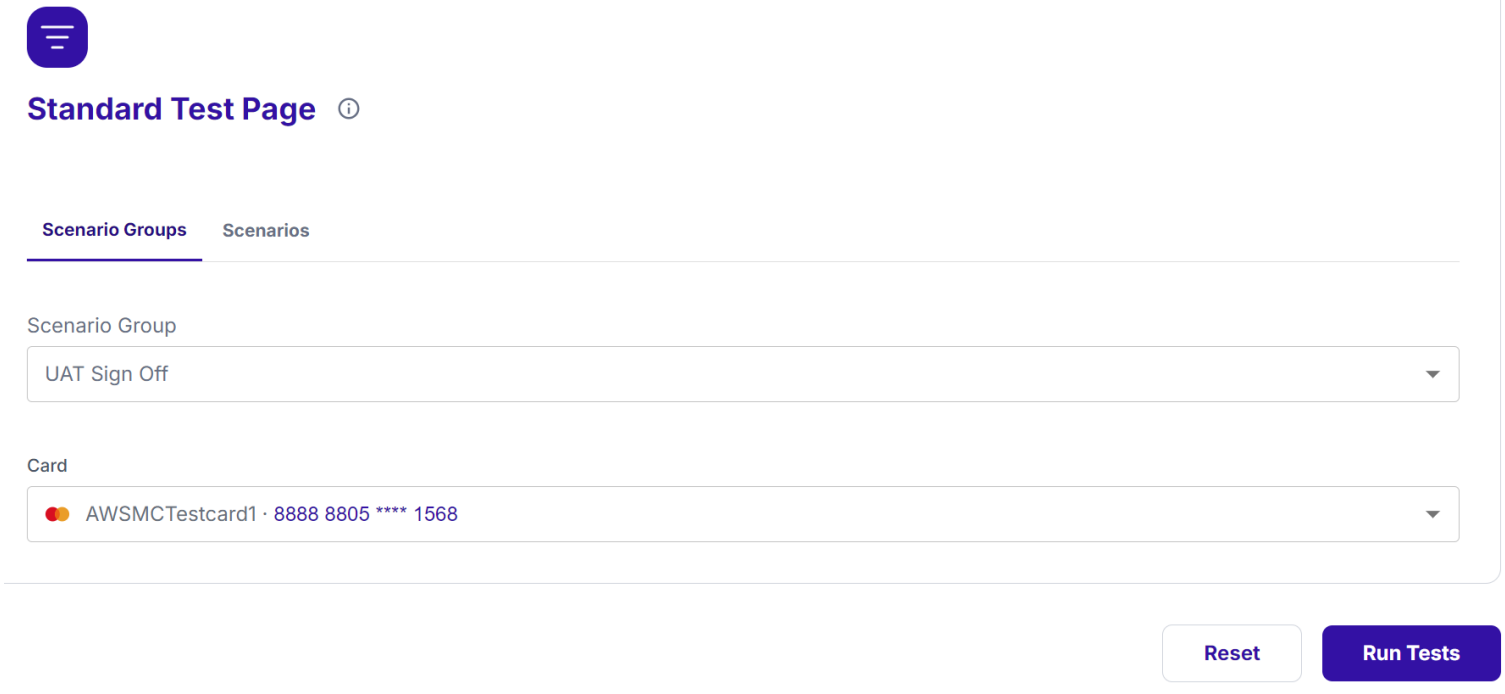


Figure 21: Running standard tests - using predefined test cases

2. Select the card you want to run the test against from the **Card** field.
3. Click **Run Tests**.

The tests in the list start running one by one with the current status shown for each. When you click the Run Test, the tests in the list start running one by one and status are shown (on the Status field). You can see the duration it took for the test to complete on the Run Time field.

Utilities

The Utils section, at the bottom of the Home page, enables you to analyse raw messages, decode messages and compare transaction data.

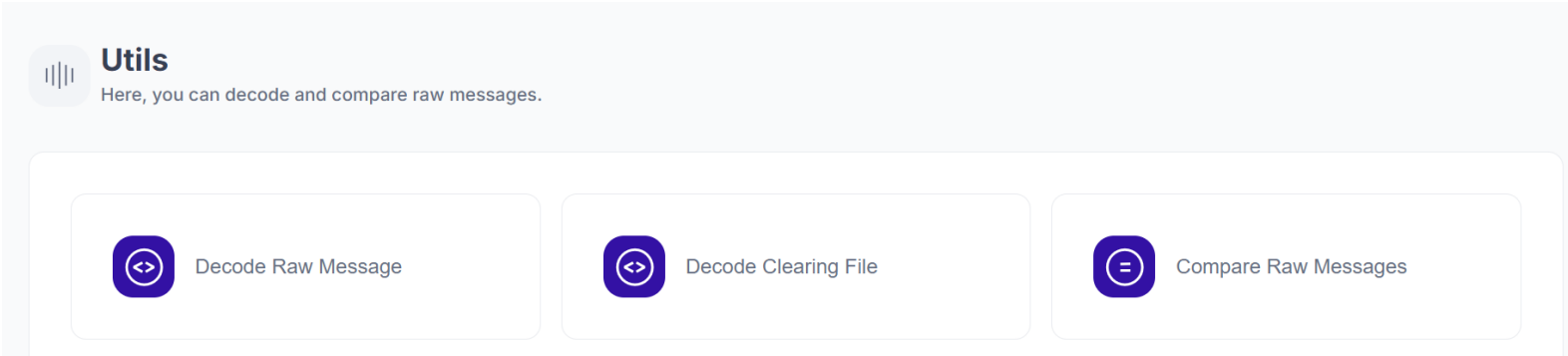


Figure 22: Analysing raw messages in the Utils section

Decode Raw Messages

To decode raw messages:

1. Click **Decode Raw Message**.
2. Paste your raw message in the Raw Message field.
3. Select the appropriate payment network.
4. Click **Decode**.

Decode Clearing File

The platform supports clearing files from multiple networks, allowing users to decode files specific to Mastercard (IPM), Visa (ITF), and Discover file types.

To decode a clearing file:

1. Click **Decode Clearing File**.
2. Click **Upload File**.
3. Search for the file you want to upload using the File Explorer.
4. Select the appropriate file type from the File Type field.
5. Click **Decode**.

Compare Raw Messages

Users can compare two different raw messages side by side to identify similarities and differences in transaction data. This feature is useful for debugging and verifying transaction consistency across different networks.

To compare raw messages:

1. Click **Compare Raw Messages**.
2. Paste the different raw messages in the Raw Message fields.
3. Select the appropriate network.
4. Enable the **Check All Fields** check box if required.
5. Click **Compare**.

5 Example Test Scenarios

The following section describes example test cases in the Payment Simulator Tool. The example test scenarios are:

- Authorisation Purchase
- Authorisation Cash Withdrawal
- Authorisation Purchase Refund
- Authorisation Purchase Recurring
- Authorisation with Tokenised Card
- STIP Advice
- Multiple Partial Reversal
- AFD - Pre-Authorisation Completion Advice
- Full Presentment Reversal After Authorisation
- Partial Presentment Reversal after Authorisation
- Chargeback Reversal after Authorisation
- Incremental Authorisation
- Non-Financial Balance Enquiry
- Non-Financial PIN Unblock
- Non-Financial PIN Change
- Non-Financial Account Status Inquiry
- Financial (Single) Purchase
- Financial (Single) Cash Withdrawal
- Financial (Single) Purchase Refund
- Multi-Currency
- Presentment Reversal
- Chargeback
- Chargeback Reversal
- Second Presentment
- Final Authorisation
- Reversal Advice

Note: You must have a valid card set up before working through a test scenario. See Cards for more information.

Authorisation Purchase

The following example test scenario covers the process of how to run an Authorisation Purchase test. The authorisation process is a crucial part of the payment lifecycle, where the card issuer approves or declines the transaction based on the cardholder's available funds and account status.

1. Navigate to the Customised Test Page.
2. Click Authorisation to begin the process. The Authorisation window displays.
3. Select **Ecommerce** from the Interface field.
4. Select **Purchase** from the Transaction Type field.
5. Select a card from the Select Card field.
6. Enter a test amount for the transaction in the Amount field. You can also add additional card-related details, such as CVV and Expiry Date if required.
7. Click **Run Test**.
8. Click View Result to review the outcome of the test.
9. Review the Test Result Modal. This displays the following information:
    - **Request Field Details**: Information about the original transaction request sent to the network.
    - **Response Fields and Details**: The response from the network, indicating whether the transaction was approved or declined.
    - **Raw Format of Request and Response Messages**: View the raw transaction data as it was sent and received between the acquirer and the issuer.
10. Return to the Test Lifecycle Overview screen.

Authorisation Cash Withdrawal

The following example test scenario covers the process of performing an Authorisation Cash Withdrawal. This process simulates the authorisation of a cash withdrawal transaction.

1. Navigate to the Customised Test Page.
2. Click Authorisation to begin the process. The Authorisation window displays.
3. Select either **Contact Chip** or **Contactless** from the Interface field.
4. Select **Cash Withdrawal** from the Transaction Type field.
5. Select the appropriate acquiring environment, card, and currency from the Acquiring Environment, Select Card and Currency fields respectively.
6. Enter the withdrawal amount in the Amount field.
7. Click **Run Test**.

Authorisation Purchase Refund

The following example test scenario covers the process of performing an Authorisation Purchase Refund. This test simulates a refund where the cardholder receives funds back into their account after a purchase, typically in response to a returned product or a cancelled service.

1. Navigate to the Customised Test Page.
2. Click Authorisation to begin the process. The Authorisation window displays.
3. Select either **Ecommerce** from the Interface field. This simulates a refund for an online transaction where the cardholder is not physically present.
4. Select **Purchase Refund** from the Transaction Type field.
5. Select the appropriate acquiring environment, card, and currency from the Acquiring Environment, Select Card and Currency fields respectively.
6. Enter the refund amount in the Amount field.
7. Click **Run Test**.

Authorisation Purchase Recurring

The following example test scenario covers the process of performing an Authorisation Purchase Recurring. Recurring payments are used for transactions that occur on a regular basis, such as subscriptions or monthly services.

1. Navigate to the Customised Test Page.
2. Click Authorisation to begin the process. The Authorisation window displays.
3. Select either **Ecommerce** from the Interface field. This simulates a recurring online transaction where the cardholder is not present.
4. Select **Purchase Recurring** from the Transaction Type field.
5. Select the appropriate acquiring environment, card, and currency from the Acquiring Environment, Select Card and Currency fields respectively.
6. Enter the recurring amount in the Amount field.
7. Click **Run Test**.

Authorisation with Tokenised Card

The following example test scenario covers the process of performing an Authorisation with Tokenised Card. Tokenised card transactions enhance security by replacing sensitive card details with tokens.

1. Navigate to the Customised Test Page.
2. Click Authorisation to begin the process. The Authorisation window displays.
3. Select either **Ecommerce** or **Contactless** (these interfaces provide transactions to wallet cards) from the Interface field. This simulates an online transaction where the cardholder is not present.
4. Select **Purchase** from the Transaction Type field.
5. Select the appropriate acquiring environment and currency from the Acquiring Environment and Currency fields respectively.
6. Enter the recurring amount in the Amount field.
7. Select a tokenised card from the Select Card field (tokenised cards display a **(Tokenised)** suffix).
8. Select a wallet for the tokenised card from the Select Wallet field.
9. Click **Run Test**. When the test is complete, a modal displays the test status. This includes the Test Status, Test Reference ID and details on the test steps. Either close the modal, click View Result to inspect the detailed response and request logs, or click Show Life Cycle to return to the full test lifecycle overview.

STIP Advice

The following example test scenario covers the process of performing a Multiple Partial Reversal test. STIP is a critical fallback mechanism that allows the network to approve or decline transactions when the primary issuer's systems are unavailable.

1. Navigate to the Customised Test Page.
2. Click STIP Advice to begin the process. The STIP Advice window displays.
3. Select **Ecommerce** from the Interface field. This simulates an online transaction where the cardholder is not present.
4. Select **Purchase** from the Transaction Type field.
5. Select the appropriate acquiring environment, card and currency from the Acquiring Environment, Select Card, and Currency fields respectively.
6. Enter the amount of the transaction in the Amount field.
7. Enter a reason code for the transaction in the Reason Code field. This code provides additional context about why the transaction is being processed using STIP.
8. Select whether STIP is set to Accepted or Declined depending on the scenario you want to test.
9. Click **Run Test**. When the test is complete, a modal displays the test status. This includes the Test Status, Test Reference ID and details on the test steps. Either close the modal, click View Result to inspect the detailed response and request logs, or click Show Life Cycle to return to the full test lifecycle overview.

Multiple Partial Reversal

The following example test scenario covers the process of performing a Multiple Partial Reversal test. A partial reversal is used to reverse a portion of the original transaction amount. In many scenarios, such as returns or corrections, multiple partial reversals may be required to adjust the authorised amount.

1. Navigate to the Customised Test Page.
2. Complete an Authorisation step. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
3. Click **Partial Reversal**. The Partial Reversal window displays.
4. Enter the reversal amount in the Amount field.
5. Click Run Test. The platform automatically calculates the remaining balance after the first partial reversal by subtracting the reversal amount from the total authorised amount. Ensure that the remaining balance is correct before moving on to the next reversal.
6. Review the balance and click Close to proceed.
7. Click Partial Reversal to display a menu, then click Additional Reversal.
8. Enter the reversal amount in the Amount field.
9. Click Run Test. Repeat steps 7 to 9 for as many reversals as required.

AFD - Pre-Authorisation Completion Advice

The following example test scenario covers the process of performing an Automated Fuel Dispenser (AFD) test. The Completion Advice step clears the transaction and prepares it for final settlement after the authorisation.

1. Navigate to the Customised Test Page.
2. Click Completion Advice to begin the process. The Completion Advice window displays.
3. Enter the amount that will be cleared for final settlement in the Amount field. This step finalises the transaction, ensuring that the correct amount is processed for settlement.
4. Click **Run Test**. When the test is complete, a modal displays the test status. This includes the Test Status, Test Reference ID and details on the test steps. Either close the modal, click View Result to inspect the detailed response and request logs, or click Show Life Cycle to return to the full test lifecycle overview.

Automated Fuel Dispenser (AFD) Completion Advice is the final step in the transaction lifecycle where the transaction amount is confirmed, and the payment is processed for settlement. This step follows the authorisation and clears the funds for the merchant.

Full Presentment Reversal after Authorisation

The following example test scenario covers the process of performing a Full Presentment Reversal after Authorisation test. Full Presentment Reversal completely reverses the presentment.

1. Navigate to the Customised Test Page.
2. Complete an Authorisation step. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
3. Click **Presentment**. The Partial Reversal window displays.
4. Complete the presentment.
5. Click Present Reversal (Full). The Presentment Reversal Full window displays.
6. Enter the reversal amount in the Amount field.
7. Click Run Test. The platform automatically calculates the remaining balance after the first partial reversal by subtracting the reversal amount from the total authorised amount. Ensure that the remaining balance is correct before moving on to the next reversal.

Partial Presentment Reversal after Authorisation

The following example test scenario covers the process of performing a Partial Presentment Reversal after Authorisation test. Partial Presentment Reversal reverses part of the presentment.

1. Navigate to the Customised Test Page.
2. Complete an Authorisation step. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
3. Click **Presentment**. The Partial Reversal window displays.
4. Complete the presentment.
5. Click Present Reversal (Partial). The Presentment Reversal Partial window displays.
6. Enter the reversal amount in the Amount field.
7. Click Run Test. The platform automatically calculates the remaining balance after the first partial reversal by subtracting the reversal amount from the total authorised amount. Ensure that the remaining balance is correct before moving on to the next reversal.

Chargeback Reversal after Authorisation

The following example test scenario covers the process of performing a Chargeback Reversal after Authorisation test. A Chargeback Reversal initiates the chargeback process for a transaction.

1. Navigate to the Customised Test Page.
2. Complete an Authorisation step. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
3. Click **Presentment**. The Partial Reversal window displays.
4. Complete the presentment.
5. Click Chargeback. The Chargeback window displays, showing the First Presentment Date and the Days Elapsed since the transaction.
6. Enter the chargeback amount, select a reason code, and enable Is Arbitration if needed.
7. Click Run Test.
8. Click Download File to download the test files.
9. Select from one of the following options:
    - Chargeback Reversal (Full) for a full reversal of the chargeback
    - Chargeback Reversal (Partial) for a partial reversal of the chargeback
    - Second Presentment to present the transaction with a new amount

Incremental Authorisation

The following example test scenario covers the process of performing a Incremental Authorisation test. Incremental Authorisation allows you to increase the amount of a previous authorisation without initiating a completely new transaction. This process is crucial for scenarios where the final transaction amount may be higher than the initial authorisation, such as in hospitality or car rental industries.

The rules for Incremental Authorisation are:

For MasterCard:

- DE061.7 = 4
- DE048.63 of following incremental preauthorisations are the combination of initial authorisation DE063 + DE015
- DE48.61 = 00001 for Incremental Final

For Visa:

- Field 63.3 = 3900
- Field 62.2 of following incremental authorisations are same as original

For both schemes, the following authorisations must match with a previous authorisation, which are not cleared (no clearing presentment record is received) and not reversed).

1. Navigate to the Customised Test Page.
2. Complete an Authorisation step. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
3. Expand the completed Authorisation step and click **Incremental Auth**. The Second Authorisation window displays.
4. Enter the incremental amount in the Amount field. You only need to enter the incremental amount, not the total transaction amount.
5. Click Run Test.
6. Review the test life cycle, then click Close.
7. Expand the Authorisation step to display the original (View Results-1) and incremental authorisation (View Results-2) test results.
8. Click View Results-2 to view details of the test. You can switch between the previous authorisation test results and the new incremental authorisation results to compare and validate both.

Non-Financial Balance Enquiry

The following example test scenario covers the process of performing a Balance Enquiry through a Non-Financial ATM test.

1. Navigate to the Customised Test Page.
2. Click Non-Financial to access Non-Financial transaction options.
3. Click Non-Financial. The Non-Financial window opens.
4. Select **Balance Enquiry** from the Transaction Type field.
5. Select a card from the Select Card field. Supported card types include MNE, Visa and MasterCard.
6. Click Run Test.
7. Click View Result to review the results displayed on completion to ensure accuracy.

Non-Financial PIN Unblock

The following example test scenario covers the process of performing a PIN Unblock through a Non-Financial ATM test.

1. Navigate to the Customised Test Page.
2. Click Non-Financial to access Non-Financial transaction options.
3. Click Non-Financial. The Non-Financial window opens.
4. Select **PIN Unblock** from the Transaction Type field.
5. Select a card from the Select Card field. Supported card types include Visa and MasterCard.
6. Click Run Test.
7. Click View Result to review the results and to confirm the PIN was successfully unblocked.

Non-Financial PIN Change

The following example test scenario covers the process of performing a PIN Change through a Non-Financial ATM test.

1. Navigate to the Customised Test Page.
2. Click Non-Financial to access Non-Financial transaction options.
3. Click Non-Financial. The Non-Financial window opens.
4. Select **PIN Change** from the Transaction Type field.
5. Select a card from the Select Card field. Supported card types include Visa and MasterCard.
6. Enter the existing PIN for the card in the Existing PIN field, and the new PIN for the card in the New PIN field.

   Note: Ensure the new PIN follows any specified security requirements, such as length and character restrictions.
7. Click Run Test.
8. Click View Result to review the results and to confirm the PIN was successfully changed.

Non-Financial Account Status Inquiry

The following example test scenario covers the process of performing an Account Status Inquiry through a Non-Financial eCOMM test.

1. Navigate to the Customised Test Page.
2. Click Non-Financial to access Non-Financial transaction options.
3. Click Non-Financial. The Non-Financial window opens.
4. Select **Account Status Inquiry** from the Transaction Type field.
5. Select an appropriate acquiring environment from the Acquiring Environment field.
6. Select a card from the Select Card field. Supported card types include Visa and MasterCard.
7. Enter the address details for the card using the Street Address and Postal Code fields.

   Note: Ensure that the entered address details match the records associated with the selected card.
8. Click Run Test.
9. Click View Result to review the results and to confirm the accuracy of Account Status information.

Financial (Single) Purchase

The following example test scenario covers the process of performing a Financial Purchase transaction through a Financial (Single) eCOMM test.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.

Financial (Single) Purchase with STIP Advice

The following example test scenario covers the process of performing a Financial Purchase transaction through a Financial (Single) eCOMM test, followed by STIP Advice.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click STIP Advice. The STIP Advice window opens.
9. Enter the amount and reason code in the Amount and Reason Code fields respectively.
10. Select whether the STIP advice is accepted by either clicking the Accepted or Declined radio box.
11. Click Run Test.

Financial (Single) Purchase with Partial Reversal

The following example test scenario covers the process of performing a Financial Purchase transaction through a Financial (Single) eCOMM test, followed by a Partial Reversal.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click Partial Reversal. The Partial Reversal window opens.
9. Enter the amount and for the partial reversal.
10. Click Run Test.

Financial (Single) Purchase with Full Reversal

The following example test scenario covers the process of performing a Financial Purchase transaction through a Financial (Single) eCOMM test, followed by a Full Reversal.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click Full Reversal. The Full Reversal window opens.
9. Enter the amount and for the full reversal.
10. Click Run Test.

Financial (Single) Purchase with Completion Advice

The following example test scenario covers the process of performing a Financial Purchase transaction through a Financial (Single) eCOMM test, followed by Completion Advice.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click Completion Advice. The Completion Advice window opens.
9. Enter the amount and for the completion advice.
10. Click Run Test.

Financial (Single) Cash Withdrawal

The following example test scenario covers the process of performing a Cash Withdrawal transaction through a Financial (Single) ATM, POS test.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Cash Withdrawal** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click Completion Advice. The Completion Advice window opens.
9. Enter the amount and for the completion advice.
10. Click Run Test.

Financial (Single) Purchase Refund

The following example test scenario covers the process of performing a Cash Withdrawal transaction through a purchase refund transaction through a Financial (Single) eCOMM, POS test.

1. Navigate to the Customised Test Page.
2. Click Single to access Single transaction options.
3. Click Financial. The Financial window opens.
4. Select **Purchase Refund** from the Transaction Type field.
5. Select an MNE card from the Select Card field. Only MNE is supported for the Single transaction.
6. Enter the amount of the transaction in the Amount field, the card's CVV in the CVV field, and the card's expiry date in the Expiry Date field.
7. Click Run Test.
8. Click Completion Advice. The Completion Advice window opens.
9. Enter the amount and for the completion advice.
10. Click Run Test.

Multi-Currency

The following example test scenario covers the process of performing a Multi-Currency transaction test through the Authorisation step in the Customised Dual Test page. Multi-Currency testing validates the system's ability to handle transactions in different currencies, ensuring compliance with international standards.

1. Navigate to the Customised Test Page.
2. Enter the details of the authorisation, including the Interface, Transaction Type, Card and Amount.
3. Enter an appropriate Transaction Type and Acquiring Environment in the relevant fields.
4. Select a suitable currency from the Currency field. Ensure the selected currency is supported by your card.
5. Click Run Test.

Presentment Reversal

The following example test scenario covers the process of performing a Presentment Reversal test (Partial or Full) using the Customised Dual Test page. Presentment Reversal testing (Partial or Full) ensures the accuracy of the reversal process in handling previously completed transactions.

1. Navigate to the Customised Test Page.
2. Click Presentment. The Presentment window opens.
3. Enter the details for the transaction, including the interface, card and amount.
4. Click Run Test.
5. Select either Presentment Reversal (Full), or Presentment Reversal (Partial). A window will open.
6. Enter the reversal amount in the Amount field. Ensure the value adheres to the reversal type selected (Partial or Full). For a Partial Reversal, ensure the entered value is less than the original transaction amount.
7. Click Run Test.

Chargeback

The following example test scenario covers the process of performing a Chargeback test using the Customised Dual Test page. The Chargeback test validates the system's capability to handle Chargeback scenarios, including arbitration.

1. Navigate to the Customised Test Page.
2. Click Presentment. The Presentment window opens.
3. Enter the details for the transaction, including the interface, card and amount.
4. Click Run Test.
5. Click Chargeback. The Chargeback window opens.
6. Enter the chargeback details, including the amount and reason. Ensure that the amount entered matches the eligible transaction value for chargeback.
7. Select the Is Arbitration radio button to specify the arbitration status for the Chargeback. Marking arbitration determines if the chargeback will proceed to an arbitration phase for resolution.
8. Click Run Test.

Chargeback Reversal

The following example test scenario covers the process of performing a Chargeback Reversal test using the Customised Dual Test page. The Chargeback Reversal test ensures proper handling and validation of reversal scenarios, whether Full or Partial.

1. Navigate to the Customised Test Page.
2. Click Presentment. The Presentment window opens.
3. Enter the details for the transaction, including the interface, card and amount.
4. Click Run Test.
5. Click Chargeback. The Chargeback window opens.
6. Enter the chargeback details, including the amount and reason. Ensure that the amount entered matches the eligible transaction value for chargeback.
7. Select the Is Arbitration radio button to specify the arbitration status for the Chargeback. Marking arbitration determines if the chargeback will proceed to an arbitration phase for resolution.
8. Click Run Test.
9. Select either Chargeback Reversal (Full) or Chargeback Reversal (Partial).
10. Enter the reversal amount in the Amount field. Ensure that the value aligns with the parameters of the original transaction and is appropriate for the selected reversal type (Full or Partial).
11. Click Run Test.

Second Presentment

The following example test scenario covers the process of performing a test for a Second Presentment test. The Second Presentment test verifies proper handling of chargebacks and disputes through subsequent transaction representation.

1. Navigate to the Customised Test Page.
2. Click Presentment. The Presentment window opens.
3. Enter the details for the transaction, including the interface, card and amount.
4. Click Run Test.
5. Click Chargeback. The Chargeback window opens.
6. Enter the chargeback details, including the amount and reason. Ensure that the amount entered matches the eligible transaction value for chargeback.
7. Select the Is Arbitration radio button to specify the arbitration status for the Chargeback. Marking arbitration determines if the chargeback will proceed to an arbitration phase for resolution.
8. Click Run Test.
9. Click Second Presentment.
10. Enter the amount of the second presentment in the Amount field. Ensure the value aligns with the previous transaction steps.
11. Click Run Test.

Final Authorisation

The following example test scenario covers the process of performing a test for Final Authorisation test. Final Authorisation confirms the total transaction amount after an initial authorisation and is only applicable to MasterCard transactions. This process is essential in industries like hospitality and car rentals, where the final amount may exceed the initial authorisation.

The rules for Final Authorisation are:

- DE061.7 = 4
- DE048.63 of following incremental preauthorisations are the combination of initial authorisation DE063 + DE015
- DE48.61 = 00001 for Incremental Final

To test Final Authorisation:

1. Navigate to the Customised Test Page. For Final Authorisation, you must have completed an authorisation test. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
2. Expand the completed Authorisation and click Incremental Auth from the menu. The Second Authorisation window opens.
3. Enter the final additional amount in the Amount field.
4. Click the Is Incremental Final? button to set this as the final authorisation.
5. Click Run Test.
6. Click Chargeback. The Chargeback window opens.
7. Enter the chargeback details, including the amount and reason. Ensure that the amount entered matches the eligible transaction value for chargeback.
8. Select the Is Arbitration radio button to specify the arbitration status for the Chargeback. Marking arbitration determines if the chargeback will proceed to an arbitration phase for resolution.
9. Click Run Test.
10. Click Second Presentment.
11. Enter the amount of the second presentment in the Amount field. Ensure the value aligns with the previous transaction steps.
12. Click Run Test.

Reversal Advice

The following example test scenario covers the process of performing a test for Reversal Advice, where you can reverse a previously completed transaction. This is particularly useful in scenarios where a transaction needs to be cancelled or corrected. The Reversal Advice process ensures that the original transaction is properly reversed in the system.

1. Navigate to the Customised Test Page. For Reversal Advice, you must have completed an authorisation test. For examples of an authorisation, see Authorisation Purchase, Authorisation Cash Withdrawal or Authorisation Purchase Refund.
2. Click Full Reversal. The Full Reversal window opens.
3. Click Is Reversal Advice? button.
4. Click Run Test.
5. Click View Result to view the result of the test. For VISA and MasterCard, ensure that the MTID is 0420 when Reversal Advice is selected, and the MTID is 0400 when only a Full Reversal is performed.

6 Appendix A: Standard Test Recommendations

The following tables describe standard test examples that Thredd recommends for each network.

Visa

The following table describes example test scenario combinations for Visa networks.

Applicable Life-Cycle	Interface Used	Terminal Types Used	Transaction Types
Dual	Magstripe	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Fallback to Magstripe	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Contact Chip	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Contactless	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Ecommerce	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	Manual Key Entry	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Mail Order	MAN	Purchase Purchase Refund Purchase Recurring Reversal
Dual	Telephone Order	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Card on File	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	E-commerce\Contactless	None	Partial Reversal Full Reversal

Applicable Life-Cycle	Interface Used	Terminal Types Used	Transaction Types
			Presentment Presentment Reversal Chargeback Chargeback Reversal Second Presentment
Non-Financial	Non Financial	ATM	PIN Unblock PIN Change Balance Inquiry
Non-Financial	Tokenisation	None	Tokenisation Authorisation Request TCN TEN
Non-Financial	Non-Financial	ECOMM	Account Status Enquiry
Tokenisation	None	None	TAR ACN TCN TEN

Mastercard

The following table describes example test scenario combinations for Mastercard networks.

Applicable Life-Cycle	Interface Used	Terminal Types Used	Transaction Types
Dual	Magstripe	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Fallback to Magstripe	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Contact Chip	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Contactless	ATM POS POS_BRANCH	Cash Withdrawal Purchase Purchase Refund
Dual	Ecommerce	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	Manual Key Entry	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Mail Order	MAN	Purchase Purchase Refund Purchase Recurring Reversal
Dual	Telephone Order	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Card on File	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	E-commerce\Contactless	None	Partial Reversal Full Reversal Presentment Presentment Reversal Chargeback Chargeback Reversal

Applicable Life-Cycle	Interface Used	Terminal Types Used	Transaction Types
			Second Presentment
Non-Financial	Non Financial	ATM	PIN Unblock PIN Change Balance Inquiry
Non-Financial	Non-Financial	ECOMM	Account Status Enquiry
Non-Financial	Tokenisation	None	TER TAR TCN TEN ACN
Tokenisation	None	None	TER TAR TCN TEN ACN

Discover

The following table describes example test scenario combinations for Discover networks.

Applicable Life-Cycle	Interface Used	Terminal Types Used	Transaction Types
Dual	Ecommerce	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	Manual Key Entry	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Mail Order	MAN	Purchase Purchase Refund Purchase Recurring Reversal
Dual	Telephone Order	MAN	Purchase Purchase Refund Purchase Recurring
Dual	Card on File	ECOM	Purchase Purchase Refund Purchase Recurring
Dual	E-commerce\Contactless	None	Partial Reversal Full Reversal Presentment

General FAQs

This section provides answers to frequently asked questions.

Q: What is the Payment Simulator Tool, and who is it intended for?

The Payment Simulator Tool is a comprehensive solution designed to help clients launch and manage payment programs efficiently. It facilitates end-to-end testing of API configurations, card processing rules, payment interfaces, and system integrations while minimizing customer impact. This tool is primarily aimed at Program Managers and developers who need to test system integrations and validate their setup before going live in a production environment.

Q: How do I sign up and log in to the Payment Simulator Tool?

To sign up to the Payment Simulator Tool:

1. Visit the login page at https://thredd.inspiriontech.co.uk/login.
2. Provide a valid email address and create a password that meets security requirements (at least 8 characters, including one uppercase letter, one lowercase letter, one number, and one special character).
3. Confirm your password and submit your registration.
4. Activate your account by following the instructions in the activation email sent to you.
5. When activated, you can log in using your credentials.

Q: What features are available on the Payment Simulator Tool dashboard?

The dashboard provides access to:

- **Homepage**, which has shortcuts for running tests and configuring settings.
- **Customised Tests**: Simulate a full lifecycle of card payment transactions with tailored test cases.
- **Standard Tests**: Run predefined test cases specific to your company.
- **Configurations**: Manage test inputs like acquirers, merchants, cards, and devices.
- **Settings**: Create and manage user accounts.

Q: How can I add a new user to the Payment Simulator Tool?

To add a new user:

1. Navigate to the **Settings** section and click **Add User**.
2. Enter the user's details (e.g. name, email address).
3. Assign a role:
    - User: Limited access to specific test features like customised and standard tests.
    - Admin: Full access to manage configurations and user settings.
4. Click **Create** to finalise user creation.

Q: What types of tests can I perform using the Payment Simulator Tool?

The tool supports various test types:

- **Customised Tests**: Simulate complete card payment transaction lifecycles with tailored scenarios (e.g., authorisation, reversals).
- **Standard Tests**: Use predefined test cases applicable to your organization.
- **Dual Message Tests**: Simulate two-step processes like authorization followed by clearing.
- **Single Message Tests**: Test single-step transactions from start to finish.
- **Non-Financial Tests**: Validate operations like tokenization or updating credentials without monetary transactions.

These tests ensure comprehensive validation of payment systems before deployment.

Document History

This section provides details of what has changed since the previous document release.

Version	Date	Reason	Revised by
1.0	06/03/2025	First version	JB

Glossary

This page provides a list of glossary terms used in this guide.

#

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as ‘Verified by Visa’ and ‘Master-card SecureCode’ respectively.

A

Acquirer

The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.

Authentication

This includes checks to confirm the cardholder identity, such as PIN, CVV2 and CAVV.

Authorisation

Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.

Automated Fuel Dispenser (AFD)

Automatic fuel dispensers (AFDs) are used at petrol or gas stations for customer self-service fuel payments. Typically the customer inserts their card and enters a PIN number and the AFD authorises a fixed amount (e.g. £99). Once the final payment amount is known, the AFD may reverse the authorisation and/or request a second authorisation.

C

Card Scheme (Network)

Card network, such as Discover, MasterCard, or Visa, responsible for managing transactions over the network and for arbitration of any disputes.

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.

Clearing File/Clearing Transaction

receive batch clearing files from the card networks, containing clearing transactions, such as presentments and network fees. The card issuer transfers the requested settlement amount to the acquirer and 'clears' the amount on the card, reducing the available card balance accordingly.

E

EMV

EMV originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit chips, in addition to mag-netic stripes for backward compatibility.

External Host

The external system to which sends real-time transaction-related data. The URL to this system is configured within per programme or product. The Program Manager uses their external host system to hold details of the balance on the cards in their programme and per-form transaction-related services, such as payment authorisation, transaction matching and reconciliation.

F

Fee Groups

Groups which control the card transaction authorisation fees, and other fees, such as recurring fees and web service API fees.

H

Hanging Filter

The period of time during which waits for an approved authorisation amount to be settled. This is defined at a product level. A typical default is 7 days for an auth and 10 days for a pre-auth.

I

Incremental Authorisation

A request for an additional amount on a prior authorisation. An incremental authorisation is used when the final amount for a transaction is greater than the amount of the original authorisation. For example, a hotel guest might register for one night, but then decide to extend the reservation for additional night. In that case, an incremental authorisation might be performed in order to get approval for additional charges pertaining to the second night.

Issuer (BIN Sponsor)

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

M

Merchant

The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.

Merchant Category Code (MCC)

A unique identifier of the merchant, to identity the type of account provided to them by their acquirer.

MIP

Mastercard Interface Processor (MIP) The processing hardware and software system that interfaces with Mastercard's Global Payment System communications network.

O

Offline Transaction

This is often used in scenarios where the merchant terminal is not required to request authorisation from the card issuer (for example for certain low risk, small value transactions used by airlines and transport networks). The card CHIP EMV determines if the offline transaction is permitted; if not supported, the terminal declines the transaction. Note: Since the balance on the card balance is not authorised in real-time, there is a risk that the card may not have the amount required to cover the transaction.

P

Partial Amount Approval

Some acquirers support a partial amount approval for Debit or Prepaid payment authorisation requests. The issuer can respond with an approval amount less than the requested amount. The cardholder then needs to pay the remainder using another form of tender.

Program Manager

A customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.

S

sFTP

Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client

Smart Client is 's user interface for managing your account on the Thredd Platform. It is also called Smart Processor . Smart Client is installed as a desktop application and requires a VPN connection to systems in order to be able to access your account.

SSL Certification

An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic with SSL/TLS, including the public key, the issuer of the certificate, and the associated subdomains.

Stand In Processing (STIP)

The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your mode, may also provide STIP on your behalf, where your systems are unavailable.

T

TLS

Transport Layer Security (TLS) is a security protocol that provides privacy and data integrity for Internet communications. Implementing TLS is a standard practice for building secure web apps.

Triple DES

Triple DES (3DES or TDES), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block to produce a more secure encryption.

V

Validation

Checks to confirm the card is valid, such as CHIP cryptograms, mag-stripe data (if available) and expiry date

VROL System

Visa Dispute Resolution Online system, provided by Visa for managing transaction disputes.

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd Ltd.

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.