more than money

# NAB Gateway Token Migration

# User Guide

April 2026 Version 1.0

# Table of Contents

# 1. Introduction

NAB Gateway, powered by Cybersource (a Visa solution) gives you one place for your online and virtual payment solutions and services. As part of NAB Gateway implementation, NAB will work with you to help ensure a smooth and successful transition of your customer card payment information for the purpose of tokenisation.

NAB will work with the Cybersource team to ensure your card payment information is securely transferred to NAB Gateway and new tokens are created.

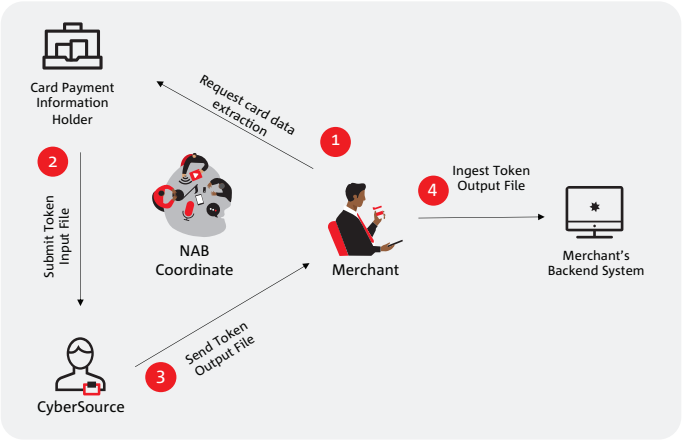
If you are a current NAB Transact merchant, moving to NAB Gateway and would like to use the Token Migration Service, you will need to contact your NAB business banker or our Transactional Banking Specialist Team to understand the process that applies to you.

## 1.1 What is Token Migration

Token migration is the activity of transferring card payment information from a merchant's current gateway to NAB Gateway and creating new tokens. This enables the merchant to continue to process payments with minimal impact to their customers and business. There are two approaches:

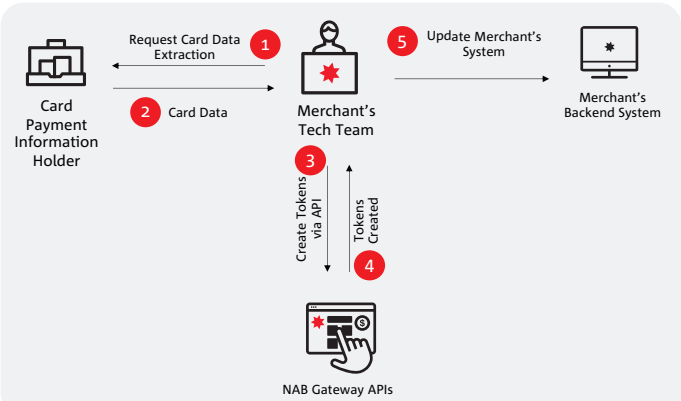
**Standard** – a file-based approach where card payment information will need to be extracted and transferred to NAB Gateway.

**Standard (File Based) Token Migration Approach**




**Self-serve** – Application Programming Interface (API) based, where a custom script or application will need to be created to call upon the required NAB Gateway APIs to create tokens in bulk.

**Self Serve (API Based) Token Migration Approach**




## 1.2 Account Updater Service

The Account Updater Service, available for both standard and self service token migration, is an optional feature that can be enabled during the token migration process, if required. The service will be disabled once all token migration activities are completed.

The Account Updater Service refreshes card payment details, including the Primary Account Number (PAN), card expiry date, and account status. This ensures that accurate and up-to-date card data is available for tokenisation. Up-to-date card data may also help improve transaction success rates.

Please liaise with your NAB contact to discuss whether the Account Updater Service is required. If required, NAB will configure the service and provide guidance to support its effective use.

Refer to section 4 for more details on Account Updater Service set up.

**Note:** Account Updater Service does not guarantee 100% success rate as not all card issuers are registered with the Account Updater Service.

# 2. Standard Token Migration

## 2.1 Prerequisites

Before commencing the standard token migration process, the following must be completed:

- A valid PCI certificate (PCI DSS SAQ type must be SAQ-D) from your card payment information holder must be provided to NAB.
- NAB Gateway facilities have been established in accordance with the Letter of Offer you have received from NAB.

## 2.2 Step by Step Instructions

### 2.2.1 Scoping meeting

Once the prerequisites are completed, a Token Migration case will be raised by NAB to engage Cybersource. A scoping meeting will then be conducted by NAB to understand the scope, timeline and confirm the next steps.

The scoping meeting should be attended by representatives from the merchant, merchant's card payment information holder, Cybersource and NAB.

### 2.2.2 Creation of VISA Enhanced File Transfer (EFT) link

Cybersource will create a secure link and an email will be sent to the key contact of the card payment information holder. The key contact will be required to create credentials and log into the EFT link.

Refer to Appendix C: Visa EFT Instruction for details on creating credentials.

### 2.2.3 Prepare the Token Input File

The merchant will need to coordinate with their card payment information holder to prepare the Token Input File (TIF). Preparation of the TIF requires the card payment information to be extracted in the required CSV format. The card payment information holder must provide the extract of data.

Cybersource will inform the key contact from the card payment information holder of any validation errors in the TIF.

Where new tokens are created after the submission of the primary TIF, a delta (secondary) TIF can be submitted within 60 days. The delta TIF can also include any remediated errors/rejections identified from the primary TIF.

Refer to Appendix A: Token Input File Specification for details.

**Important:**

- Each file can contain up to 1 million records. Additional TIFs will be required if there are more than 1 million records.
- Perform a duplicate check before submitting your data to prevent duplicate card numbers from being migrated. The token migration process does not perform this check.
- It is recommended that card payment information, including the expiry dates are up to date, before preparing the TIF.

### 2.2.4 Encrypt the Token Input File

The card payment information holder must encrypt the TIF using the Pretty Good Privacy (PGP) public key based on the details below:

- **Key ID:** 65708434
- **Key Type:** RSA-S
- **Key Size:** 4096
- **Fingerprint:** FCF3 F156 58C4 E125 FA5B 7D57 32FA 394B 6570 8434
- **User ID:** Authorize.Net Migration

Cybersource PGP Public key is available on this link: Knowledge Article Detail Page - Visa

### 2.2.5 Upload the encrypted Token Input File via the Visa EFT Link

The card payment information holder will need to upload the encrypted TIF via the Visa EFT link.

Refer to Appendix C: Visa EFT instructions for details on how to upload the encrypted file.

### 2.2.6 Receive the Token Output File

After successful processing of the TIF, Cybersource will create a Token Output File (TOF) in CSV format and send to the nominated email address belonging to the merchant. This file includes new NAB Gateway tokens linked to the original customer profile ID provided in the TIF.

Refer to Appendix B: Token Output File Specification for details.

**Note:** Failures will be noted in the Token Output File. The 'remarks' field in the TOF will include a reason for the failure or rejection. Rectified data can be submitted via a delta TIF within 60 days of submitting the primary TIF.

### 2.2.7 Ingest the Token Output File

The data in the TOF must be used to update token data in the merchant's backend system(s) in readiness to commence transactions.

### 2.2.8 Submit a delta (secondary) Token Input File, if required

The delta TIF can include tokens created after the submission of the primary TIF and any remediated errors/rejections identified from the primary TIF. A further Token Output File will be generated by Cybersource and sent to the nominated email address belonging to the merchant.

# 3. Self-Serve Token Migration

## 3.1 Prerequisites

Before commencing, the following must be completed:

- A valid PCI certificate (PCI DSS SAQ type must be SAQ-D) from the party performing the process to create tokens using APIs i.e. merchant or card payment information holder, must be provided to NAB.
- NAB Gateway facilities have been established in accordance with the Letter of Offer you have received from NAB.
- Access to NAB Gateway API credentials established. Refer to the next section for details.

## 3.2 Access to NAB Gateway API credentials

The merchant (admin user) will need to create the required API authentication credentials to be used for integration with NAB Gateway. Alternatively, the admin user can create a 'developer/technical support' role to provide access. This enables their technical team to create credentials to authenticate and integrate with NAB Gateway. The instructions for creating and assigning roles are available from the NAB Gateway Support centre.

When setting up the role, assign the permission group 'payment configuration permissions' which allows the technical team to generate the credentials (shared secret key or P12 certificate) required for authentication with NAB Gateway and process APIs.

To connect successfully, the merchant's system must be able to communicate using REST APIs. For more information and instructions on setting up REST APIs, visit the NAB Developer Centre.

## 3.3 API Endpoints & Authentication Methods

All API requests are sent via HTTP to these endpoints:

- Sandbox (Testing): https://nabgateway-api-test.nab.com.au
- Production (Live): https://nabgateway-api.nab.com.au

You can choose between two authentication methods:

- JSON Web Token (JWT)
- HTTP Signature Messaging

More information is available on NAB Developer Centre page for API Endpoint and Authentication.

## 3.4 Testing

Use the NAB Gateway Sandbox environment and the provided test card numbers to validate your integration.

- Use any future expiry date.
- Use any 3-digit CVV for Visa/Mastercard, and 4-digit for Amex.
- Please find test card numbers: Testing Guide | NAB Developer Portal

## 3.5 Step by Step Instructions

The API options listed are to create a single token per card per API. For bulk token creation, a custom script or application will need to be developed by the merchant's tech team to automatically call the required NAB Gateway APIs.

### 3.5.1 Option 1: Using multiple Token Management Service (TMS) APIs

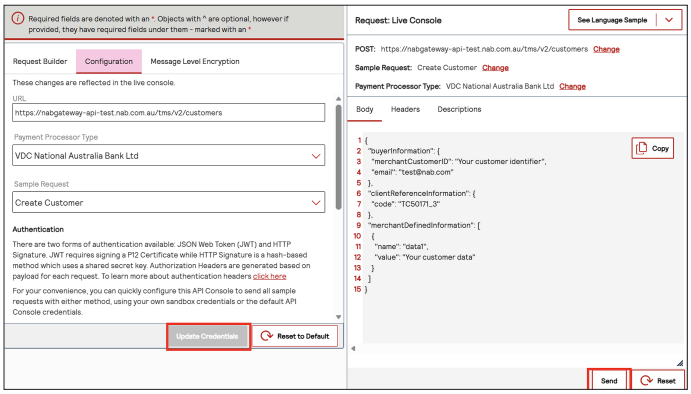
This option requires the use of multiple APIs such as – Customer ID, Instrument Identifier and Payment Instrument to create tokens. The mandatory customer card payment information required to successfully create tokens is: PAN (card number), expiry date and billing information.

To create gateway tokens using TMS APIs, follow these steps:

**Step 1: Register the customer in NAB Gateway**

API: Create Customer ID

This creates the Customer ID which would be required in Step 3.

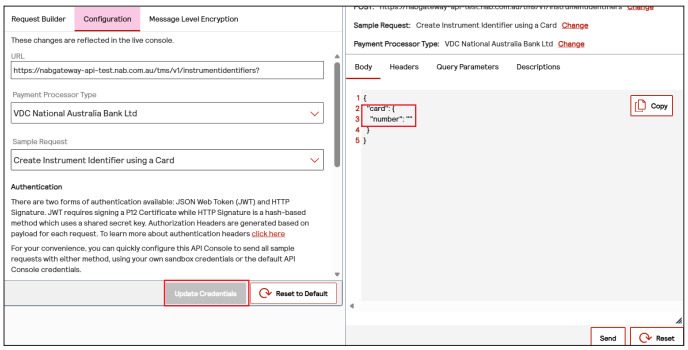



**Note:** Click on 'Update Credentials' before pressing 'Send' for each step. After each step, a success message should appear.

**Step 2: Convert PAN to token**

API: Create Instrument Identifier

This creates the instrument identifier which will also be required in Step 3.



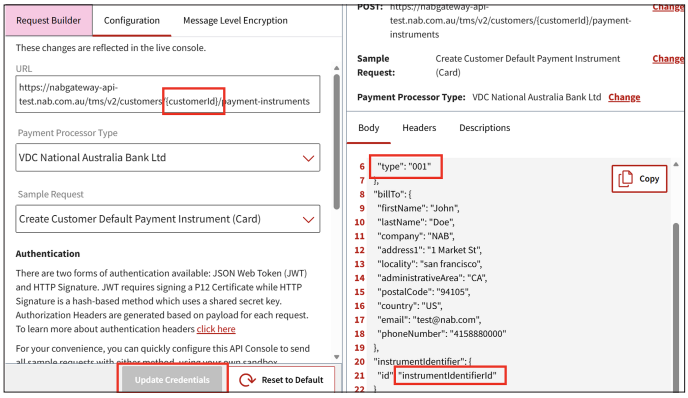
**Step 3: Associate the Instrument Identifier token with the customer profile.**

API: Create Customer Payment Instrument

Enter in the Customer ID created in Step 1 in the 'URL' field

Enter in the Instrument Identifier created in Step 2 in the "instrumentIdentifier" field.

Enter in the code under 'type' according to the card type. Note that in the 'Request Builder' section, 'Card' then 'Type' there is a list of the various cards and what the code should be.

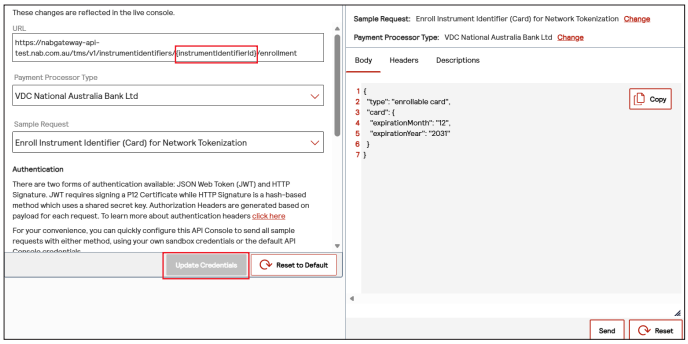



**Step 4: To provision a Network token for an existing Instrument Identifier**

API: Enrol an Instrument Identifier for Payment Network Token

Enter in the Instrument Identifier in the URL.

Click on 'Update Credentials' before pressing 'Send'.




## 3.5.2 Option 2: Using $0 Authorisation Payment APIs

This option includes processing a $0 authorisation payment with token creation using a single API. A successful transaction will create the Customer ID, Payment Instrument and Instrument Identifier tokens. Please ensure valid card payment information details are provided for tokens to be created successfully.

Upon a successful transaction, a Transaction Identifier (TID) or Processor Transaction ID will be generated. This ID is used to track the transaction lifecycle and should be included in subsequent recurring transactions if applicable, to continue with recurring payments.

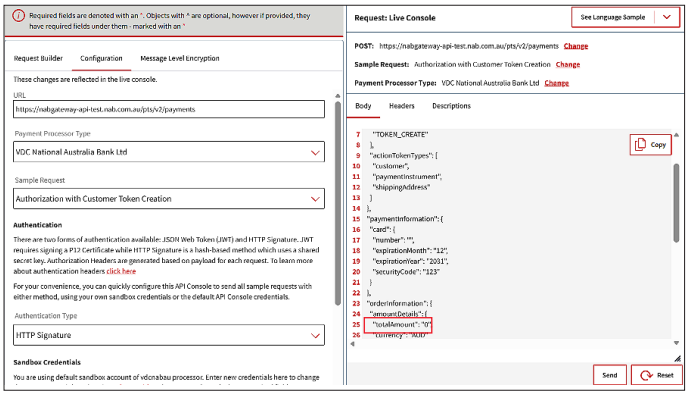
Network tokens will be created if network tokenisation has been enabled on the merchant's NAB Gateway account.

**Note:** Transaction fees will apply to $0 auth payments.

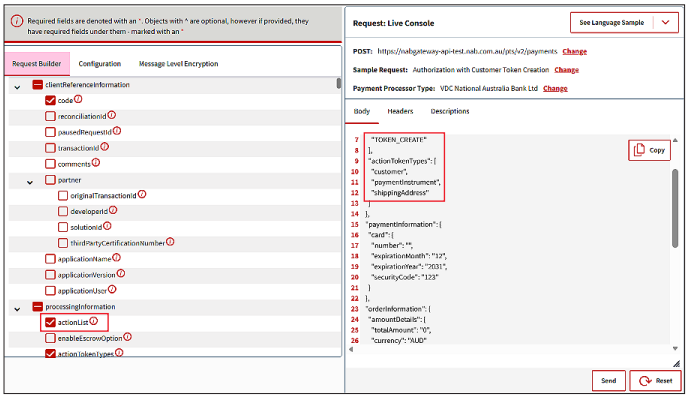
To create NAB Gateway tokens via $0 authorisation payment, follow these steps:

API: Authorization with Customer Token Creation API

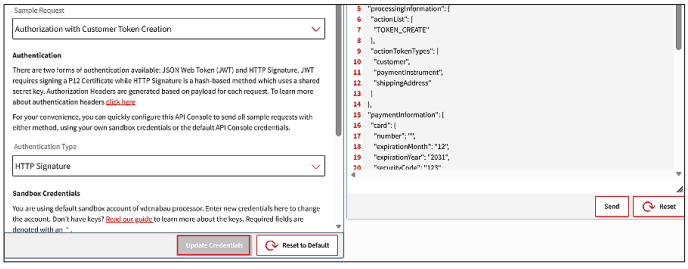
**Step 1: Change the value of "totalAmount" to 0**




**Step 2: Add "actionList" under 'Request Builder' section**




**Step 3: Click on 'Update Credentials' before you click on 'Send'. You should see a 'Success' message appear.**




## 3.5.3 View tokens created in NAB Gateway Portal

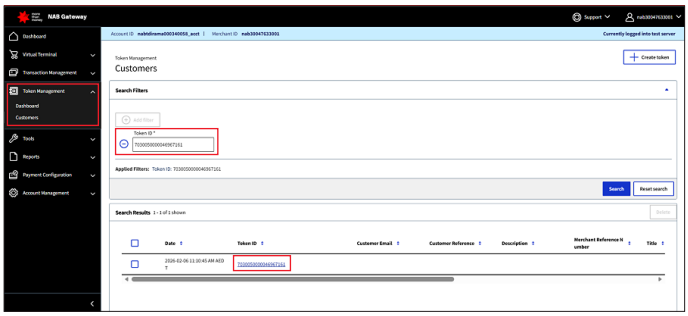
Confirm a token has been successfully created using APIs by following these steps:

**Step 1: Login to NAB Gateway Portal**

**Step 2: Go to 'Token Management'**

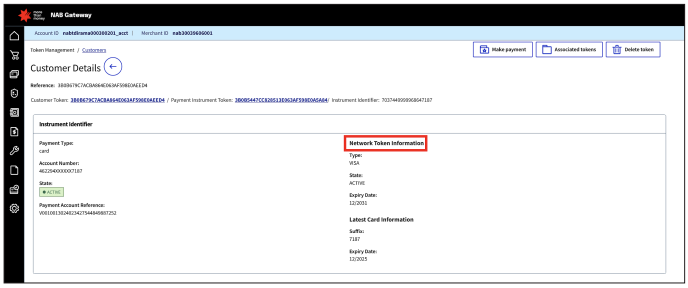
**Step 3: Go to 'Customer'**

## Step 4: Search by ‘Token ID’ which is the Customer ID created




Click on either the Customer ID or Instrument Identifier and the following screen should appear.


**Note:** if a network token has been created, it will appear as follows.



# 4. Optional Service

## 4.1 Account Updater Guide

### 4.1.1 Register Your Account Updater Service

Provide the required information listed below to the NAB team managing Token Migration.

For Visa and Mastercard, the merchant's contact information is required. For Mastercard only, a technical contact must also be provided.

Merchant Contact Information

- Name:
- Title:
- Email:
- Phone:

Technical Contact Information

- Name:
- Title:
- Email:
- Phone:

Note that the enrolment process can take up to 10 business days.

For American Express, the AMEX SE number will need to be provided to the NAB team to configure Account Updater. If an AMEX SE number is not available, the merchant will need to contact AMEX to have a SE number organised.

### 4.1.2 Account Updater Configuration

Once the merchant is registered with required schemes for the Account Updater Service, NAB will configure Account Updater Service on your merchant facility. The Account Updater Service enables merchants to submit tokenised cards to Visa and Mastercard for updates on an agreed date. AMEX updates are run daily by default.

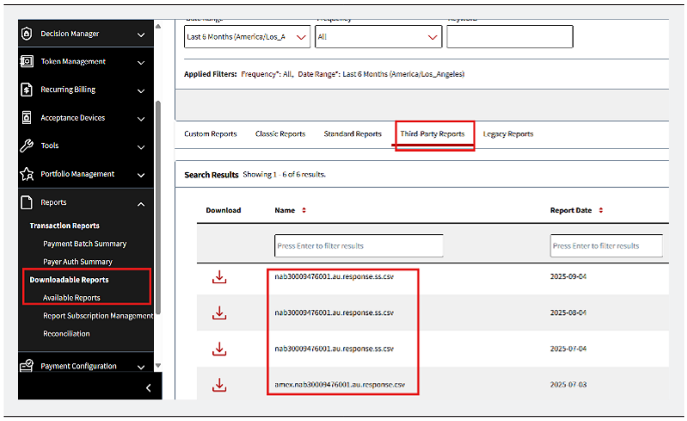
Important: The Account Updater Service is configured at the Transacting MID (TMID) level and can only request updates for NAB Gateway tokens created for that TMID. If a merchant has multiple TMIDs with tokens, Account Updater Service must be configured for each TMID.

### 4.1.3 Download the Account Updater Report

Once Account Updater has been configured in the NAB Gateway Portal, an Account Updater report can be downloaded to review the outcome, if required.

Go to 'Under Reports' > 'Available Reports' > Third-Party Reports section: (refer to the screenshot)

| Third-Party Reports | Descriptions |
|---|---|
| <merchantID>.au.response.ss.csv | Visa & Mastercard Account Updater report |
| Amex.<merchantID>.au.response.ss.csv | Amex Account Updater report |




### 4.1.4 Analyse an Account Updater Report

#### 4.1.4.1 Understand Account Updater Report Format

The format for a response file consists of these components:

- A header record
- A detail record with one or more data records, each on a separate line
- A footer record, which indicates the end of the file

The record consists of comma-separated values and uses the fields listed in the following:

| Header Record | | | |
|---|---|---|---|
| **Field Name** | **Sample Value** | **Description** | **Data Type & Length** |
| Record Identifier | H | Constant value indicating the record type.<br>Format: **H** | Alpha (1) |
| File Classification | cybs.au.response.pan | Indicates that this is a request or response file, and the type of service.<br>Format: cybs.au.response.pan | Alphanumeric (30) |
| MerchantID | Nab1234567891011 | Your merchant ID. | Alphanumeric (30) |
| BatchID | 12233344445555566666777777788 | File (batch) identifier sent in the request file | Numeric (30) |
| **Response Detail Record** | | | |
| **Field Name** | **Sample Value** | **Description** | **Data Type & Length** |
| Record Identifier | D | Constant value indicating the record type.<br>Format: **D** | Alpha (1) |
| Request ID | 1000000000000000002 | Unique identifier for the record. | Numeric (30) |
| Old Card Number | 22223XXXXX5555 | Old card number | Numeric (19) |
| Old Card Expiration Month | 11 | Old expiration month.<br>Format: MM | Numeric (2) |
| Old Card Expiration Year | 24 | Old expiration year.<br>Format: YY | Numeric (2) |
| New Card Number | 666677XXXXX9999 | New card number. | Numeric (19) |
| New Card Expiration Month | 11 | New expiration month.<br>Format: MM | Numeric (2) |
| New Card Expiration Year | 26 | New expiration year.<br>Format: YY | Numeric (2) |
| Merchant Reference ID | | This field is optional and is returned in the response if present in the request file | Alphanumeric (50) |
| BA Sub Merchant ID | | This field is returned in the response if sent in the request file | Alphanumeric (10) |
| Response Code | NAN | Response code for the record. | Alpha (3) |
| Reason Code | 800 | Reason code for the record | Numeric (3) |
| **Response Footer Record** | | | |
| **Field Name** | **Sample Value** | **Description** | **Data Type & Length** |
| Record Identifier | F | Constant value indicating the record type.<br>Format: **F** | Alpha (1) |
| Record Count | 2 | The number of detail records in the file. | Numeric (10) |
| Response Code | COM | Response code for the file. | Alpha (3) |
| Reason Code | 800 | Reason code for the file | Numeric (3) |

#### 4.1.4.2 Understand Response Codes and Reason Codes

- **Record Level:**

The response code and the reason code for the record appear in the details record of the request file.

Response Codes and Reason Codes:

| Response Code | Response Code Description | Reason Code | Reason Code Description | Billable or Non-Billable Code |
|---|---|---|---|---|
| ACL | Match: account closed. The state of the Instrument Identifier token gets set to Closed. | 800 | Success. | Billable. |
| CCH | Contact card holder. | 800 | Success. | Billable. |
| CUR | Card data current. | 800 | Success. | Non-billable. |
| DEC | n/a | 801 | Invalid card number. | Non-billable. |
| DEC | n/a | 802 | Invalid check digit. | Non-billable. |
| DEC | n/a | 803 | Invalid expiration date. | Non-billable. |
| DEC | n/a | 804 | Unsupported card type | Non-billable. |
| DEC | n/a | 805 | Invalid card type length. | Non-billable. |
| DEC | n/a | 806 | Unknown card type. | Non-billable. |
| DEC | n/a | 810 | Invalid BA sub merchant ID. | Non-billable. |
| DEC | n/a | 850 | Invalid token format. | Non-billable. |
| DEC | n/a | 851 | Invalid token length | Non-billable. |
| DEC | n/a | 852 | Unknown token.<br>This token does not exist, is not associated with your account, or might be superseded. | Non-billable. |
| DEC | n/a | 853 | Invalid token status.<br>This token has a status of CLOSED from a previous Account Updater batch. | Non-billable. |
| DEC | n/a | 861 | Cardholder is already enrolled or cannot cancel cardholder that is not enrolled. | Non-billable. |
| DEC | n/a | 862 | Rejected because cardholder opted out. | Non-billable. |
| ERR | n/a | 801 | Invalid card number. | Non-billable. |
| ERR | n/a | 802 | Invalid check digit. | Non-billable. |
| ERR | n/a | 803 | Invalid expiration date. | Non-billable. |
| ERR | n/a | 804 | Unsupported card type or cancelled card. | Non-billable. |
| ERR | n/a | 807 | Merchant not enrolled properly in Account Updater. | Non-billable. |
| ERR | n/a | 808 | Incorrect record indicator | Non-billable. |
| ERR | n/a | 809 | Unknown error code received during processing | Non-billable. |
| ERR | n/a | 811 | New account number failed MOD-10 check. | Non-billable. |
| NAN | New account number. It might also include a new expiration date. | 800 | Success. | Billable. |

| Response Code | Response Code Description | Reason Code | Reason Code Description | Billable or Non-Billable Code |
|---|---|---|---|---|
| NED | New expiration date | 800 | Success. | Billable. |
| NUP | No match, no update. | 800 | Success. | Non-billable. |
| UNA | Inconsistent update received, not applicable. | 800 | Inconsistent update received, not | Non-billable. |

**Request File Level:**

The response code and the reason code for the request file appear in the footer record of the request file.

Request File Response Codes and Reason Codes

| Response Code | Response Code Description | Reason Code | Reason Code Description |
|---|---|---|---|
| COM | The merchant request file has been validated, processed, and the response received | 800 | Success. |
| DEC | The merchant request file was not processed because each record failed record-level validation. | 801 | Success. |

# 5. Frequently Asked Questions

## 5.1 Standard Token Migration

### 5.1.1 How many Token Input Files can I submit for processing?

One Token Input File can include a maximum of 1 million tokens. The number of primary Token Input Files will depend on your token volume. In addition, you can also submit a delta file to cover additional tokens created after your primary Token Input File was submitted. This can also contain updated or corrected card payment information that failed or were rejected in the primary Token Input File.

### 5.1.2 What if my card data is incomplete or outdated?

It is recommended that you have up to date card payment information to avoid token creation and transaction failures.

If outdated or incorrect card payment information is transferred to NAB Gateway you can opt for the Account Updater Service, which may help in updating the card payment information.

Important note: Account Updater Service does not guarantee 100% success rate as all card issuers may not be registered with the Account Updater Service.

### 5.1.3 I've enrolled in the Account Updater Service so why haven't my AMEX tokens been updated?

This may be due to creation of a new AMEX SE number during NAB Gateway onboarding. The new AMEX SE number must be linked to your old AMEX SE number in AMEX system to ensure the AMEX tokens are updated using the Account Updater Service.

### 5.1.4 What if I want to convert gateway tokens to network tokens and how?

If network tokenisation is enabled on your account, the first successful transaction using a gateway token will automatically create a network token.

If you have a need to convert gateway tokens to network tokens in bulk, please speak to your NAB contact.

### 5.1.5 How many tokens can I migrate?

There is no limit to the number of tokens you can migrate. The limitation applies to the Token Input file, which can contain up to 1 million tokens. If you are looking to migrate over 1 million tokens, you will need to submit multiple token input files.

## 5.2 Self-Serve Token Migration

### 5.2.1 Can I use batch APIs for token migration?

No, NAB Gateway does not currently support batch APIs. You'll need to develop a custom script or application to automate bulk token creation using the available APIs.

### 5.2.2 Where can I find sample codes for integration?

Please find GitHub Samples via: Cybersource · GitHub

# 6. Appendix A – Token Input File (TIF) Specification

The table below outlines the Token Input File Specification. Please request the template from your NAB contact if needed.

| Field Number | Field Name | Mandatory / Optional |
|---|---|---|
| 1 | customer.tokenid* (current Customer ProfileID) | Mandatory |
| 2 | card.number | Mandatory |
| 3 | card.exp_month | Mandatory |
| 4 | card.exp_year | Mandatory |
| 5 | card.id (payment profile ID associated with Customer ProfileID) | Optional |
| 6 | customer.email | Optional |
| 7 | card.billto.first_name | Optional |
| 8 | card.billto.last_name | Optional |
| 9 | card.billto.company | Optional |
| 10 | card.billto.address | Optional |
| 11 | card.billto.address2 | Optional |
| 12 | card.billto.city | Optional |
| 13 | card.billto.state | Optional |
| 14 | card.billto.zip | Optional |
| 15 | card.billto.country | Optional |
| 16 | card.billto.phoneNumber | Optional |
| 17 | card.merchant_initiated_transaction.previous_transid | Optional for token migration<br>Mandatory if doing recurring MIT (Merchant Initiated Transaction). If not available, further discussion is required to determine workarounds. |

# 7. Appendix B – Token Output File (TOF) Specification

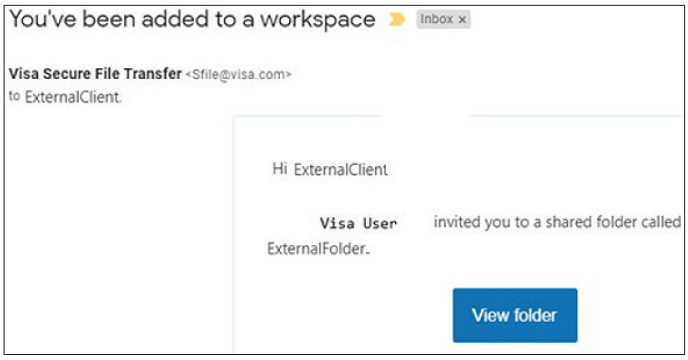
The table below outlines the Token Output File Specification. Please request the template from your NAB contact if needed.

| Field Number | Field Name | Description |
|---|---|---|
| 1 | OldCustomerProfileId | This will be the value assigned to your customer by your previous provider |
| 2 | TmsCustomerTokenId | This ID will be assigned to your customer in your account |
| 3 | OldPaymentProfileId | This will be the value assigned to your customer's payment information by your previous provider. |
| 4 | TmsPaymentInstrumentId | This ID will be assigned to your customer's payment information in your account |
| 5 | TmsInstrumentIdentifierId | Token type represents the tokenised Primary Account Number (PAN) for card payments.<br>Duplicate entries of TmsInstrumentIdentifierId could be present if multiple accounts were created with the same card or shared use across accounts |
| 6 | OldShipmentProfileId | This will be the value assigned to your customer's shipping information by your previous provider and will be empty. |
| 7 | TmsShipmentInstrumentId | This ID will be assigned to your customer's shipping information in your account |
| 8 | Remarks | In the remarks field we will let you know if any row failed to import and the reason<br>Known rejections<br>Spaces in any of the Mandatory fields<br>Card Number not Numeric<br>Expiry date older than 10 months of Migration date |

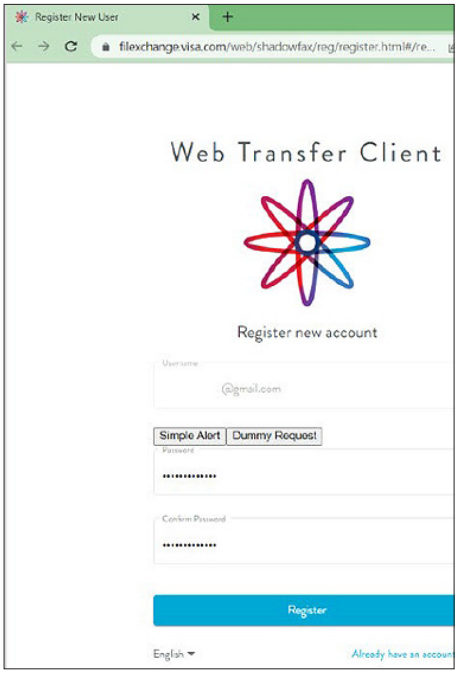
# 8. Appendix C – Visa EFT Instruction

## Set Up and Sending Files with Visa EFT

**Step 1:** An email with an invite will be sent, refer to the following screenshot:

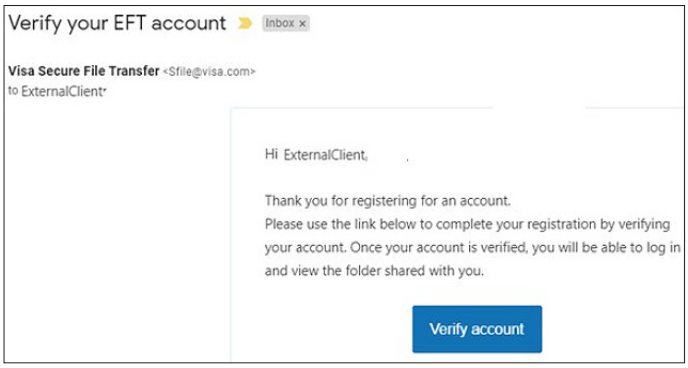



- Click the View folder button. The Web Transfer Client page should then appear.
- Fill out the fields for Password. Follow the required password complexity.
- You will receive an email notification to verify the account upon successful registration.

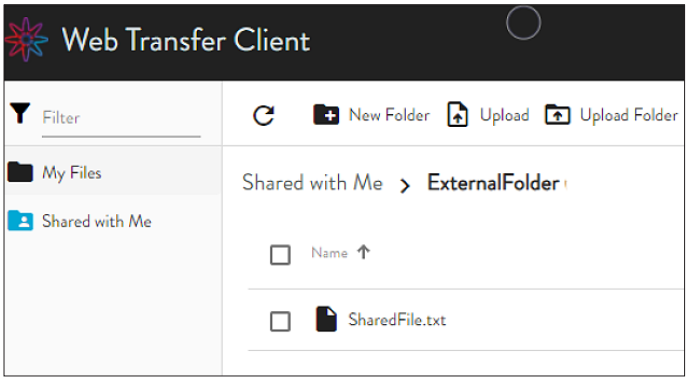



**Step 2:** Verification of the account using the email verification must be performed before accessing the Enhanced File Transfer Web page. Select Verify account in the email.

The EFT Web Transfer Client page should appear. Folders and files shared by Visa will be available for viewing.

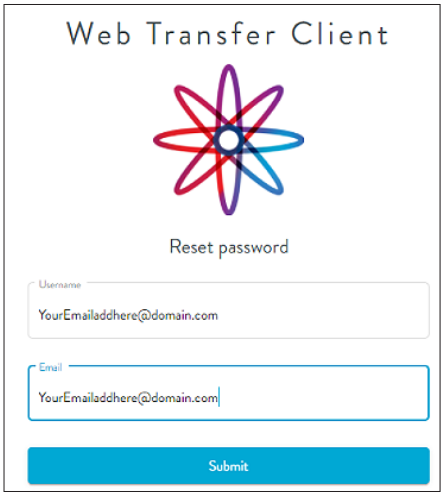



**Step 3:** Click on the Shared with Me folder on the left and then select the Folder that was shared to upload the Token Input File/s.



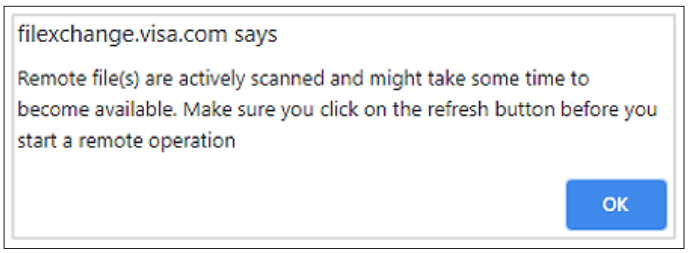

### Reset Your Password

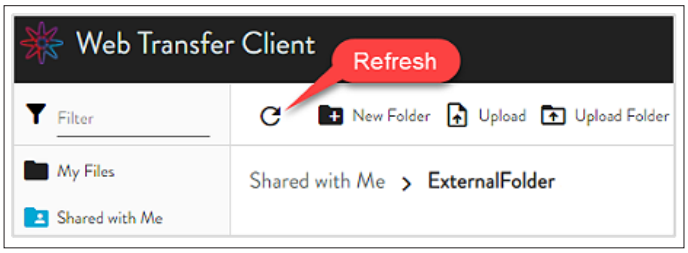
To reset password click Forgot Password on the Enhanced File Transfer login page. Make sure to type in the registered email address on both the username and email address field as shown:



**Things to Note**

- Files can only be uploaded or downloaded from the folder shared by Visa employees under the Shared with Me folder.
- The following message will be shown every time a folder is created, or a file is uploaded on the Shared with Me space. Make sure to click on the refresh button as the files are actively scanned. It may take some time for the uploaded file to become available and to appear.




Guest account (external user's account) gets disabled if it's been inactive for over 90 days. To activate the account again, request your NAB contact to coordinate with Visa to send a new EFT invitation email.