Forte Sandbox Setup

10/10/2024 3:29 pm EDT

Contents

Purpose

This document discusses how to set up a sandbox to test EFT payment processing for Forte.

It is important to note that a full test of EFT processing is not possible due to the sensitivity of the credit card and ACH information that exists within the customer's database and the high risk of generating payment information for a customer. Forte does not allow tokenization of existing EFT data under sandbox credentials. Sandbox credentials allow for adding new payment methods to the system but will not accept existing payment methods. Existing payment methods either do not have a token, or the token was generated using different credentials. When using sandbox credentials, the user will need to add new payment methods for testing.

The risk to EFT payment processing issues post SedonaOffice v5.7 to 6.x is very low, therefore we don't recommend full testing of EFT in a test environment. For customers that insist on testing EFT processing, a scenario can be set up. However, it will only allow very limited testing. These limitations include:

- Submitted transactions will not settle or reject. They will remain in the Accepted status. There is no way for a transaction submitted with sandbox credentials to emulate the settlement process.
- Since transactions will not settle, you cannot deposit batches containing these transactions.
- Previously Funded transactions will not come through so you won't be able to see practical Z-Transaction batches.

Essentially, sandbox DEX credentials allow for users to see how the EFT Processing screens looks, add new payment methods, and submit transactions. All other functions are disabled.

Return to Contents

Process Flow

The following steps will be required to set up a test for EFT processing:

1. The customer must request sandbox DEX credentials from Forte, or have Forte walk them through generating sandbox DEX credentials.

2. The live database is copied to a sandbox database
    1. If the customer is already on version 6, then they could have auto-submit enabled in their database. This would cause double submissions, as they would submit any transactions currently in the Ready status. Whenever cloning a database on version 6 or higher, ensure you take precautions when cloning the database to prevent duplicate submissions.
3. The new sandbox DEX API credentials are added to the sandbox database in EFT Setup.
    1. This occurs on the existing MID. The MID and the Organization ID remain the same, the API ID and Secure Key are updated with the sandbox information
4. Customers will need to add new test payment methods and update existing customers to that new payment method for testing.
5. Process EFT as normal

Return to Contents

Advanced Users

If someone is insistent on doing full EFT Processing, the only current way to do so is through a separate testing MID. The user would need to reach out to Forte to generate a new Merchant ID separate from their existing MID. This is not a sandbox; it would be a second production environment used for Development or Testing. If they complete this step, then the user would be able to enter a new MID into EFT Setup and test real transactions using company credit cards. Any existing payment method tokens would fail since they would not be tokenized with this new MID. The user would still need to add new payment methods for their testing, but these transactions would be live transactions and able to settle like normal.

Return to Contents

Additional Information

This is a short video by Forte on how to generate API credentials: https://www.youtube.com/watch?v=rncc-Kkm5r8

Another video by Forte on how to switch to Sandbox mode: https://www.youtube.com/watch?v=_Hwr91Pu_VY

A popup message occurs when you first swap to version 6 and also whenever you add a new MID. This is because new MIDs are not added as PCI Compliant by default. In a testing environment, you can shortcut the need to run the full PCI utility by updating the value to 'C'. This should only be done in a testing environment and never in production. However, this can cause the newly added MID to not submit transactions or have other annoying repercussions. For expediency in testing, you can run the below SQL query:

Update ar_ach_direct set PCI_Compliant = 'C'

That should set all MIDs in the test database to compliant. For production, an investigation should be undertaken to

ensure there's no real PCI information remaining after an import or other reason a new MID might be added to their database.

Return to Contents