Authorize.Net Mobile Application

iOS User Guide

September 2015
Authorize.Net LLC ("Authorize.Net") has made efforts to ensure the accuracy and completeness of the information in this document. However, Authorize.Net disclaims all representations, warranties and conditions, whether express or implied, arising by statute, operation of law, usage of trade, course of dealing or otherwise, with respect to the information contained herein. Authorize.Net assumes no liability to any party for any loss or damage, whether direct, indirect, incidental, consequential, special or exemplary, with respect to (a) the information; and/or (b) the evaluation, application or use of any product or service described herein.

Authorize.Net disclaims any and all representation that its products or services do not infringe upon any existing or future intellectual property rights. Authorize.Net owns and retains all right, title and interest in and to the Authorize.Net intellectual property, including without limitation, its patents, marks, copyrights and technology associated with the Authorize.Net services. No title or ownership of any of the foregoing is granted or otherwise transferred hereunder. Authorize.Net reserves the right to make changes to any information herein without further notice.

Authorize.Net Trademarks
Advanced Fraud Detection Suite™
Authorize.Net®
Authorize.Net Your Gateway to IP Transactions™
Authorize.Net Verified Merchant Seal™
Automated Recurring Billing™
eCheck.Net®
Contents

Recent Revisions to This Guide  5

About This Guide  6
  Audience and Purpose  6
  Conventions  6
    Note, Important, and Warning Statements  6
    Text and Command Conventions  7
  Customer Support  7

Chapter 1  Introduction  8
  Features  8
  Feedback  8

Chapter 2  Merchant Requirements  9
  Device Support  9
  Merchant Agreements  9
  Collecting Customer Information  9
  Product Type  10
  Account User Types  11
  For More Information  11

Chapter 3  Setting Up  12
  Reviewing Payment Form Settings  12
  Configuring Address Verification Service (AVS) Settings  13
  Updating Business Information  13
  Downloading the Authorize.Net Mobile Application  14
  Accepting Terms and Conditions  14
  Logging In to Your Account  14
    Using a Sandbox Account  14
Recent Revisions to This Guide

<table>
<thead>
<tr>
<th>Release</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2015</td>
<td>Updated guide to reflect the most recent enhancements to the user interface.</td>
</tr>
<tr>
<td>June 2014</td>
<td>Updated guide to indicate that application can be used with both card-not-present and card-present accounts.</td>
</tr>
<tr>
<td>April 2013</td>
<td>Added information about card readers.</td>
</tr>
</tbody>
</table>
About This Guide

Audience and Purpose

This guide is written for merchants who use the Authorize.Net mobile application to process transactions. Some operations require administrator privileges in the Authorize.Net merchant interface.

Conventions

Note, Important, and Warning Statements

A Note contains helpful suggestions or references to material not contained in the document.

An Important statement contains information essential to successfully completing a task or learning a concept.

A Warning contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.
Text and Command Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
</table>
| **bold**   | - Field and service names in text; for example: Include the *ics_applications* field.  
- Items that you are instructed to act upon; for example: Click **Save**. |
| *italic*   | - Filenames and pathnames. For example: Add the filter definition and mapping to your *web.xml* file.  
- Placeholder variables for which you supply particular values. |
| **monospace** | - XML elements.  
- Code examples and samples.  
- Text that you enter in an API environment; for example: Set the *davService_run* field to true. |

Customer Support

For support information about any Authorize.Net service, visit the Support Center:  
https://support.authorize.net/
Introduction


Features

- Uses existing Authorize.Net account login ID and password to securely access the Authorize.Net Payment Gateway through the Authorize.Net Mobile Application.
- Accepts credit, signature debit, and prepaid card payments from Visa, MasterCard, American Express, and Discover.
- Establishes settings with a simple one-time configuration that enables merchants to set a default tax rate, skip signature for transaction amounts less than $25, and turn Tips on or off.
- Itemizes individual items for purchase.
- Captures shipping details for goods to be shipped to the customer.
- Sends an email receipt of the completed transaction to the customer’s email address.
- Manages transactions originated by the device such as voids (voiding of unsettled transactions) and refunds (refunding of settled transactions).
- Tracks the history of all purchase and void/refund transactions or searches for specific transactions originated from the device.
- Securely manages and controls permissions for multiple devices.

Feedback

If you have any comments or suggestions about the Authorize.Net Mobile Application, please contact feedback@authorize.net.

If you have any comments or suggestions about this document, please contact documentation@authorize.net.
CHAPTER 2

Merchant Requirements

Device Support

The Authorize.Net Mobile Application supports devices on the Apple iOS platform version 8 or later, with connectivity from a wireless carrier or Wi-Fi provider.

Merchant Agreements

The Authorize.Net Payment Gateway Merchant Service Agreement and the Authorize.Net Mobile Application Terms and Conditions govern the use of your Authorize.Net Payment Gateway account and your use of the Authorize.Net Mobile Application, respectively. Both the agreement and the terms and conditions require you to comply, at your expense, with all laws, policies, guidelines, regulations, ordinances, orders of any governmental body and/or rules applicable to your use of the Authorize.Net services including, without limitation, the rules promulgated by the credit card networks and the Federal Trade Commission, and all laws and regulations governing the security, privacy, collection, retention and use by Merchant of consumer data, including, without limitation, financial information, card account numbers, and all other personally identifiable consumer information.

Collecting Customer Information

You may collect shipping addresses using the Authorize.Net Mobile Application only if you are shipping a product to a customer. Should you collect a customer’s shipping address or any other personally identifiable information for the purpose of shipping a product to the customer, you may not use such information for any purpose other than product shipment.

The customer’s email address can be captured only when the application prompts for it after the transaction is completed, subject to the customer’s request for an email receipt. See “Sending an Email Receipt,” page 21.
Product Type

You can use the Authorize.Net Mobile Application key-in functionality with both card-present and card-not-present accounts. You can use an encrypted card reader with either type of account. Different transaction rates apply depending on which type of transaction you process. For more information on transaction pricing, call your merchant bank and your Authorize.Net sales contact.

To view your Authorize.Net product type:

**Step 1**  Log in to your account at https://account.authorize.net.
**Step 2**  In the main toolbar, click Account.
**Step 3**  Click Merchant Profile.
**Step 4**  Under Business Information, refer to Product Type.
Account User Types

The Authorize.Net Payment Gateway account includes the following account user types:

**Account Owner**: an account owner is the top level user, has access to all features of the Merchant Interface, and manages all other user accounts. Only an account owner can create another account owner.

**Account Administrator**: by default, an account administrator has all Merchant Interface permissions except for the ability to enable or disable payment gateway services or manage account owner user accounts.

**Transaction Manager**: by default, a transaction manager can perform all transaction processing functions in the Merchant Interface.

For More Information

For more information about this product, including availability, pricing, and transaction rates, contact your merchant bank and your Authorize.Net sales contact.
Before downloading the app, you can begin by completing some mobile-related tasks in the Authorize.Net merchant interface.

### Reviewing Payment Form Settings

The Payment Form settings in the Merchant Interface enables you to specify certain fields as being required when transactions are submitted to Authorize.Net. Because the fields passed to Authorize.Net from the Authorize.Net Mobile Application are already defined, you may experience transaction errors (Reason Response Code 33) if you have other fields selected as required in the Payment Form settings. To prevent these errors, log in to the Merchant Interface and review the Payment Form settings.

**To review payment form settings:**

1. **Step 1** Log in to your account at [https://account.authorize.net](https://account.authorize.net) using your login ID and password.
2. **Step 2** From the main toolbar, click **Account**.
3. **Step 3** Under Transaction Format Settings, click **Payment Form**.
4. **Step 4** Click **Form Fields**.
5. **Step 5** Uncheck all selected fields in the Required column.
6. **Step 6** Click **Submit**.

Changes made to the Payment Form settings will affect any software solution that posts transactions to Authorize.Net using the Advanced Integration Method (AIM), Direct Post Method (DPM) or Server Integration Method (SIM). Contact your developer to ensure that other solutions are not adversely affected by these changes.
Configuring Address Verification Service (AVS) Settings

AVS helps detect suspicious payment card transactions. It compares the billing address provided by the cardholder with the billing address on file at the payment card issuing bank. A transaction is accepted or rejected based on your AVS settings in the Merchant Interface. When a transaction is rejected, the application displays a status of Declined.

**To configure your AVS settings:**

1. Log in to the Merchant Interface at https://account.authorize.net/.
2. From the main toolbar, click **Account**.
3. Select **Settings**.
4. In the Security Settings section, click **Address Verification Service**.
5. Check the AVS codes for which the payment gateway should reject transactions.
6. Click **Submit**.

Changes made to the AVS settings will affect any transaction submitted to Authorize.Net using the Advanced Integration Method (AIM), Direct Post Method (DPM) or Server Integration Method (SIM). Contact your developer to ensure that other solutions are not adversely affected by these changes.

Updating Business Information

To edit your business information, you must log in to the Authorize.Net Merchant Interface. If you have not entered merchant information in the app, the receipt will use the information entered in this section. If merchant information is entered in the app, the information in the app take precedence.

**To update your business information:**

1. Log in to the merchant interface at https://account.authorize.net/.
2. In the main toolbar, click **Account**.
3. In the left menu, click **Merchant Profile**.
4. Click **Edit Business Information**.
5. Update your business information as needed by editing the provided text fields and drop-down menus.
Step 6  Click Submit.

---

**Downloading the Authorize.Net Mobile Application**

Merchants with an Authorize.Net Payment Gateway account can obtain the application two ways:

- Download from an iOS device: obtain the application directly from Apple’s App Store using an iPhone, iPod touch, or iPad.
- Download from iTunes on a PC or Mac: using an existing iTunes account, you can download the application on a PC or Mac and then synchronize it to your iOS device.

When the download is complete, the iOS device’s home page displays an icon for the Authorize.Net Mobile Application.

**Accepting Terms and Conditions**

The first time you launch the Authorize.Net Mobile Application on your mobile device, you are prompted to accept the Terms and Conditions specific to the Authorize.Net Mobile Application. You will continue to be subject to your existing Authorize.Net Payment Gateway Merchant Service Agreement.

**Logging In to Your Account**

After you accept the Terms and Conditions, the login page appears. Enter your Merchant Interface credentials and tap Log In.

**Using a Sandbox Account**

We recommend that you test your implementation using your sandbox account before processing live transactions. Tap the Use Sandbox Account slider on the login page. When you are logged into the sandbox account, an orange bar appears at the top of the user interface.
If you do not have a sandbox account, tap the Create Sandbox Account to Try This App link.

**Allowed Special Characters**
The following table shows which special characters are allowed, and for which fields.

<table>
<thead>
<tr>
<th>Special Character</th>
<th>Login ID</th>
<th>Password</th>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>%</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>- (Hyphen)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>_ (Underscore)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>#</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>&amp;</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Authorizing the Device for Use**

After you download the Authorize.Net Mobile Application and enter your login ID and password, you will see a message indicating that use of the Authorize.Net Mobile Application on that device is pending approval.

**To approve the Authorize.Net Mobile Application for use on a device:**

**Step 1** Log on to the Authorize.Net Merchant Interface using your existing Authorize.Net login ID and password.

**Step 2** In the Account menu, choose Settings.

**Step 3** In the Security Settings section, choose Mobile Device Management. A screen appears, showing mobile devices that are active or pending approval for that account.

**Step 4** Choose the device, and click Enable Device.

**Managing Mobile Devices**

Using the Authorize.Net merchant interface, an account administrator can enable, disable, or delete mobile devices from an account.
To manage mobile devices:

**Step 1** Log in to the merchant interface at https://account.authorize.net.

**Step 2** Navigate to Account > Settings > Security Settings > General Security Settings > Mobile Device Management.

**Step 3** Select a device in the Device ID column.

**Step 4** Click one of the following options: Enable Device, Disable Device, or Delete Device.

---

**Setting Up the Application**

When you log in for the first time, the Settings page opens.

**Merchant Information**

Here you can enter information about your business that will appear on the receipt sent from the mobile device. If you do not enter information in the app, the receipt will display the merchant information that exists in the Authorize.Net merchant interface. If you enter merchant information in the app, the information in the app will supersede the information in the merchant interface.

**Fields in Merchant Information Settings**

- Business name
- Address
- City
- State
- ZIP code
- Phone number
- Email address

**Sales Tax**

Tap the slider to enable the sales tax feature. The Sales Tax page appears. Use the number dials to select the default sales tax percentage. When you are finished, tap Back to return to the Transaction Settings page.
Chapter 3  Setting Up

Tipping
Tap the slider to enable the tipping feature.

Note that when tipping is enabled, a signature is always required. Keep this requirement in mind when adjusting the Skip Signature option.

Shipping
Tap the slider to enable the shipping feature. Doing so enables you to add shipping address information. Shipping information includes:

- First name
- Last name
- Address one
- Address two
- City
- State
- ZIP code
- Phone number

Skip Signature
When this feature is enabled, a signature is not required for transactions of less than $25. Be aware that this feature is incompatible with tipping. When tipping is enabled, the Skip Signature option cannot be enabled.

Reason Response Codes
Reason Response Codes may be displayed in parentheses within the Authorize.Net Mobile Application when an error occurs during processing.

To view reasons for a specific error:

Step 1  Go to https://developer.authorize.net/tools.
Step 2  Click Response Reason Code Tool.
Step 3  Enter the error code.
Step 4  Click **Submit.**
Accepting Payments

CHAPTER 4

Using the Transaction Page

The Transaction page is where you create an itemized list of goods and services.

To create an itemized list:

Step 1  Tap Add Item. The Items page appears.
Step 2  Tap Add an item.
Step 3  Enter a description and price for the item. If you do not enter a description, the default description is Goods/Services.
Step 4  Tap Next.
Step 5  Enter a price for the item.
Step 6  Tap Done.
Step 7  To add another item, repeat Steps 1-6. When you are finished adding items, tap Back to return to the Order page.
Step 8  If shipping is enabled, tap Shipping.
   a  Enter shipping information and tap Done.
   b  Tap Set. The Order page appears.

Entering Payment Information

After creating an itemized list, you can enter payment information by either using a card reader or keying in the payment information.
To use the encrypted card reader:

Step 1  Plug the reader into the headphone jack of your mobile device.
        A warning indicates that the headphone volume must be at maximum in order to proceed.
Step 2  Tap OK.
Step 3  Swipe the card.
        The Authorize page appears.
Step 4  The customer signs in the signature area.

Important: Do not reduce or mute the volume while the card reader is plugged in to the
headphone jack. The reader draws power from your device’s headphone jack. When you plug in the reader, your device’s volume is automatically set to
maximum. If you manually decrease or mute the volume level while the
reader is plugged in, the reader might not have enough power to read credit
card data, and you will receive an error.

Completing the Transaction

From the Authorize page, the customer can do the following:

- Enter a tip amount if the Tip feature is enabled (optional)
- Confirm the final transaction amount
- Provide a signature
- Tap Authorize to complete payment

Confirmation of the Transaction

After the transaction has successfully completed, the Authorize.Net Mobile Application
displays the Transaction Summary page. A unique Transaction ID is generated and
appears with the transaction status.

After you review the Transaction Summary page, choose one of the following actions:
Send the customer an email receipt and tap Send. For more information about email receipts, see "Sending an Email Receipt," page 21.

Tap New Transaction to begin a new transaction.

If the transaction results in an error, you receive the same error codes that apply to standard Authorize.Net transactions. Refer to the online Response Reason Code Tool for further detail about these codes:

https://developer.authorize.net/tools/responsereasoncode/

### Sending an Email Receipt

A customer can provide an email address to receive a receipt by email. A customer is not required to provide this information. If a customer prefers not to provide an email address for delivery of the transaction receipt, a merchant must comply with pertinent laws and regulations and the agreement with their acquirer pertaining to the provision of receipts for debit and credit card transactions, which may include providing a paper receipt. If a customer declines to receive a receipt in any form, you do not need to provide a receipt. You may provide a handwritten receipt if requested by the customer.

The email is sent from the Authorize.Net gateway on your behalf. If the customer replies to this email, the reply is sent to the email address associated with your Authorize.Net Payment Gateway account.

---

The receipt is sent, but is not saved to your mobile device.

---

### Logging Out of the Authorize.Net Mobile Application

To log out of the application, go to the Menu page, tap Log Out, and then confirm that your want to log out.

The Authorize.Net Mobile Application automatically logs off when the Authorize.Net Mobile Application is idle for 30 minutes, and after every 8-hour interval, regardless of use.

If you use the application after it is idle for 30 minutes, you will not be asked to log in until you try to perform an action (such as send a payment from the Review & Authorize page or view the History page). If you are prompted to log in after tapping Authorize in the Review & Authorize page, you can then resume your previous session. All basket information should be available to you, but previously entered payment information will not be because this information is not stored on the device.
If you are using an iOS device without multitasking functionality, and you tap the device’s home button, the device’s home page appears and the application closes. The next time you open the application, you will have to log in using your login ID and password.
Managing Transactions

CHAPTER 5

Enabling the Transaction Details API

Before you can view transaction history from the application, you must enable transaction details in the merchant interface.

To enable the Transaction Details API:

1. Log in to your account at https://account.authorize.net.
2. Enter your login ID and password.
3. Click Account.
4. Under Security Settings, click Transaction Details API.
5. Enter your secret answer.
6. Click Enable Transaction Details API.

The default setting of the Transaction Details API feature on the Merchant Interface is OFF, which prevents you from seeing the history of transactions made with the application or from accessing the Void or Refund functions for those transactions.

If you do not enable this feature, you cannot view transaction history on the application.

Note

An owner or administrator has the ability to see Settings and History pages as part of the application’s Manage feature. If the Transaction Details API remains OFF, the owner or administrator sees only the Settings page and the Transaction Manager can see only the History page. In this case, the Transaction Manager cannot see the Manage feature.
Viewing Transaction History

You can view transactions submitted through the Authorize.Net Mobile Application from the logged-in user if you have enabled the Transaction Details API. For more information on enabling the Transaction Details API, see "Reviewing Payment Form Settings," page 12.

An account owner or account administrator can see Settings and History pages as part of the application’s Manage feature. A Transaction Manager can see only the History page, assuming the account’s Transaction Details API is enabled.

To view the transaction history, press the three-bar button on the upper-right side of the page and choose Transaction History.

You can choose the following types of transactions:

- **Last Transaction**: this option displays the details of the last transaction processed by this device.
- **Unsettled Transactions**: this option displays purchases or refunds that are pending settlement. Tap a transaction to display its details. You can void an unsettled transaction from the detail page by tapping Void.
- **Settled Transactions**: this option displays purchases that have already settled as part of the standard Authorize.Net settlement process. Tap a transaction to view its details. You can refund a transaction from the details page by tapping Refund.
- **Voided Transactions**: this option displays voided transactions, which are defined as unsettled transactions that were cancelled before settlement. Tap a transaction to view its details.
- **Refunded Transactions**: this option displays those settled transactions that were refunded to the original card. Tap a transaction to view its details.

Searching Transactions

You can search for specific transactions from the Transaction History page. Enter a valid Transaction ID, and the Details page for that transaction appears.
Deleting the Mobile Application

To delete the Authorize.Net Mobile Application from your device:

Step 1  Find the Authorize.Net Mobile Application icon on your device’s home page.
Step 2  Press and hold the icon until a small x appears in the top left corner of the icon.
Step 3  Tap the x next to the Authorize.Net Mobile Application icon.
Step 4  Tap **Delete** to delete the application and all of its data.
Supported Card Readers

Only card readers that have been injected with the Authorize.Net security key are supported. The card readers below work only with certain devices and carriers. Before purchasing, we recommend that you ensure your device and carrier are compatible before purchasing.

How to Order

Supported mobile card readers may be purchased through our partner POS Portal. For more information, visit http://authorizenet.posportal.com/.