MIVA MERCHANT

Credit Card Security and Encryption Guide

© Copyright 2005-2013, Miva Inc.

Miva®, Miva Merchant® and Miva Central® are registered trademarks of Miva Inc.

Intuit, the Intuit logo, Quicken, QuickBooks, TurboTax, Lacerte, ProSeries and QuickBase, among others, are registered trademarks and/or registered service marks of Intuit Inc., or one of its subsidiaries, in the United States and other countries.

All rights reserved. The information and intellectual property contained herein is confidential between Miva® Inc and the client and remains the exclusive property of Miva® Inc. If you find any problems in the documentation, please report them to us in writing. Miva® Inc. does not guarantee that this document is error free. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Miva® Inc.

This document, and all materials, products and postings are made available on an "as is" and "as available" basis, without any representation or warranty of any kind, express or implied, or any guaranty or assurance the document will be available for use, or that all products, features, functions or operations will be available or perform as described. Without limiting the foregoing, Miva® Inc is not responsible or liable for any malicious code, delays, inaccuracies, errors, or omissions arising out of your use of the document. As between you and Miva® Inc, you are assuming the entire risk as to the quality, accuracy, performance, timeliness, adequacy, completeness, correctness, authenticity, security and validity of any and all features and functions of the document.

The Miva Merchant® logo, all product names, all custom graphics, page headers, button icons, trademarks, service marks and logos appearing in this document, unless otherwise noted, are trademarks, service marks, and/or trade dress of Miva® Inc (the "Marks"). All other trademarks, company names, product names, logos, service marks and/or trade dress displayed, mentioned or otherwise indicated on the Web Site are the property of their respective owners. These Marks shall not be displayed or used by you or anyone else, in any manner, without the prior written permission of Miva® Inc. You agree not to display or use trademarks, company names, product names, logos, service marks and/or trade dress of other owners without the prior written permission of such owners. The use or misuse of the Marks or other trademarks, company names, product names, logos, service marks and/or trade dress or any other materials contained herein, except as what shall be permitted herein, is expressly prohibited.

Contents

BEST PRACTICES FOR MANAGING CREDIT CARD DATA 1

THE ENCRYPTION KEY WIZARD 1
ABOUT ENCRYPTING PAYMENT INFORMATION 2
ABOUT DELETING PAYMENT INFORMATION 3

ENABLING ENCRYPTION IN YOUR STORE 3

NOTES 3
TO ENABLE ENCRYPTION IN YOUR STORE 4

PROCESSING EXISTING ORDERS WITH THE ENCRYPTION KEY WIZARD 6

TO PROCESS EXISTING ORDERS WITH THE ENCRYPTION KEY WIZARD 6

REGULAR ARCHIVING IN THE MANAGE ORDERS SCREEN 10

TO ARCHIVE AN ORDER 10

TO VIEW ENCRYPTED CREDIT CARD INFORMATION 12

IN THE ORDER ENCRYPTION SCREEN 12
IN THE MANAGE ORDERS SCREEN 13
IN LEGACY ORDER PROCESSING 14

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

Best Practices for Managing Credit Card Data

A portion of the PCI-DSS standard relates to encrypting your payment data. In most cases you are required to meet these standard, although they are also considered best practices:

- **Enable encryption in your store**. After you enable encryption, payment information on new orders will be encrypted.
- **Encrypt existing payment information**. If you have existing orders with unencrypted payment information, you have to encrypt the payment information on those orders.
- **Delete payment information from orders**. PCI has several requirements for when you should delete payment information:
  - It is never acceptable to keep unencrypted credit card numbers in your database, even temporarily.
  - You should not keep credit card data longer than you need to. For example, the PCI standards let you store credit card information to cover your return policy, or if you sell custom products that may be paid for in installments. However, you should delete credit card information when you no longer need it to process or refund an order.
  - In no circumstances should you store payment information in your database for more than 1 year.
  - You may never store the entire stripe data (which includes the CVV code) even if it's encrypted.

The Encryption Key Wizard

You can do all of the tasks mentioned above with the **Encryption Key Wizard**. The Encryption Key Wizard is a utility that is part of the Miva Merchant admin interface. The main purpose of the Encryption Key Wizard is to

- Enable order encryption in your store by creating an encryption key.
- Create new encryption keys. PCI standards require you to create a new encryption key every 365 days.
- Remove payment information from orders (Archiving).

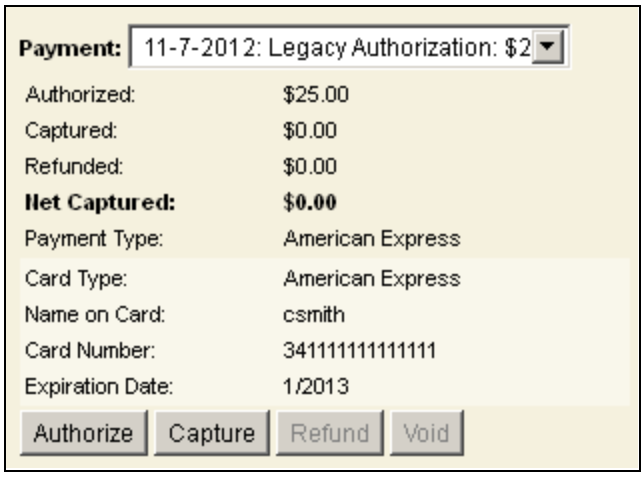
Note that the screens in the Encryption Key Wizard will be slightly different, depending on whether you have existing orders with credit card data in them.

• You don't have an encryption key. • You have an encryption key, but you don't have any orders with credit card data. The wizard will only prompt you to create a new encryption key.	• You don't have an encryption key. • You have an encryption key, and you have at least one order with credit card data. The wizard will prompt you to create a new encryption key and then allow you to:

© Copyright 2005-2013, Miva Inc. All Rights Reserved.
Publication Date: 11/21/2013 Version 1.2

	• Migrate orders (encrypt them), and/or • Archive orders (strip payment info)

About Encrypting Payment Information

	
Edit an order. Order encryption is not enabled.	Edit an order. Order encryption is enabled.

- Only the payment information is encrypted, not the entire order.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

- You can view encrypted payment information in the clear as long as you have the Passphrase to decrypt the order. It is impossible to decrypt the data without your Passphrase.
- You cannot remove encryption from existing orders. Although you can edit an order and temporarily view the payment information in the clear, once you encrypt payment information in an order, the encryption is permanent.
- Miva Merchant encryption works by having you create an encryption key. The encryption key is a long alphanumeric string that the software uses as a seed for the encryption algorithm. It's important that you have a copy of your encryption key stored somewhere securely. If you forget what your encryption key is, you won't be able to complete several tasks in Miva Merchant. Only you will know your encryption key and if you lose it or forget it, it can't be recovered, even by Miva Merchant staff.
- The PCI standards require you to create a new encryption key every 365 days.

About Deleting Payment Information

- In Miva Merchant, deleting payment information is called Archiving. Archiving doesn't remove orders from your store database. The only purpose of archiving is to strip payment information from orders.
- You can remove payment from orders in batch or from one order at a time. But once you remove payment information from an order it is permanently deleted.

Enabling Encryption in Your Store

You enable encryption in your store by creating an encryption key. As soon as you create the key, credit card data on new orders will be encrypted. You create the key with the Encryption Key Wizard.

Follow the steps in this section if you want to enable encryption in your store, and you **do not** have existing orders with credit card information.

But see also *Processing Existing Orders with the Encryption Key Wizard*.

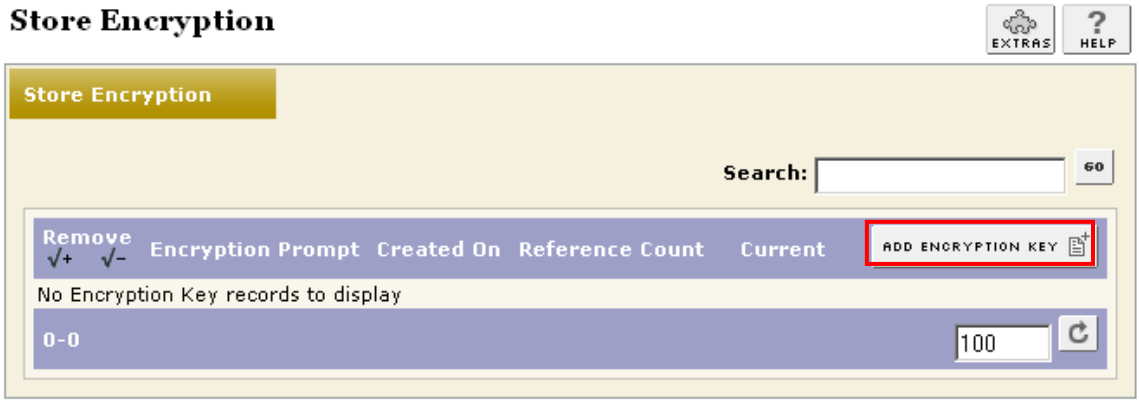
Notes

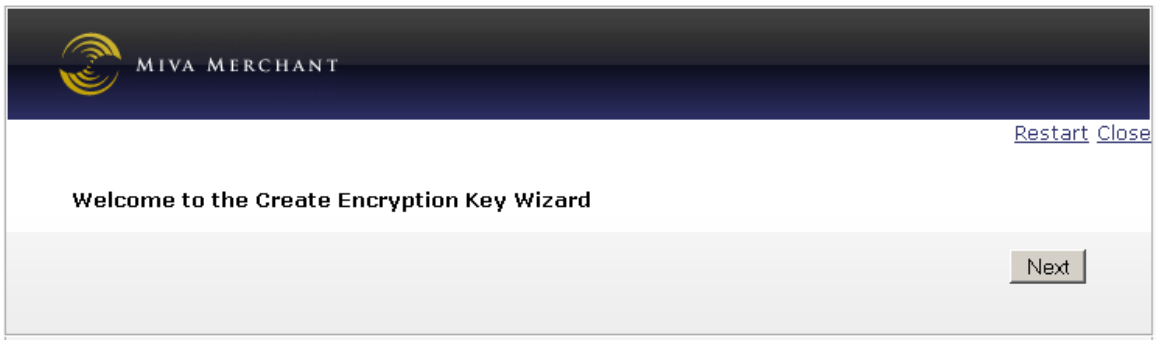
- In this section we've simplified the screens to make them easier to read.
- It's important that you make a note of your encryption key passphrase and store it in a secure location. If you lose your passphrase, it cannot be recovered. You will either have to:
  - Remove payment information from all of the orders whose credit card information was encrypted (archiving), or
  - Leave the orders with encrypted credit card information in your database. You won't be able to view the credit card information when you edit an order.

© Copyright 2005-2013, Miva Inc. All Rights Reserved. Publication Date: 11/21/2013 Version 1.2

To Enable Encryption in Your Store

1. Select Order Encryption from the leftnav.
2. In the Store Encryption main screen, click the **Add Encryption Key** button.

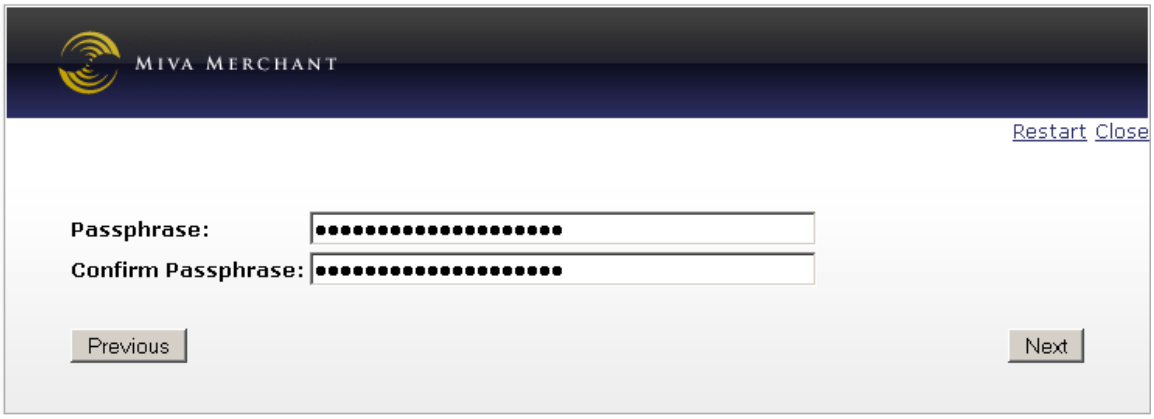




Click Next.

Enter a Prompt (a descriptive name) for the encryption key and click Next.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

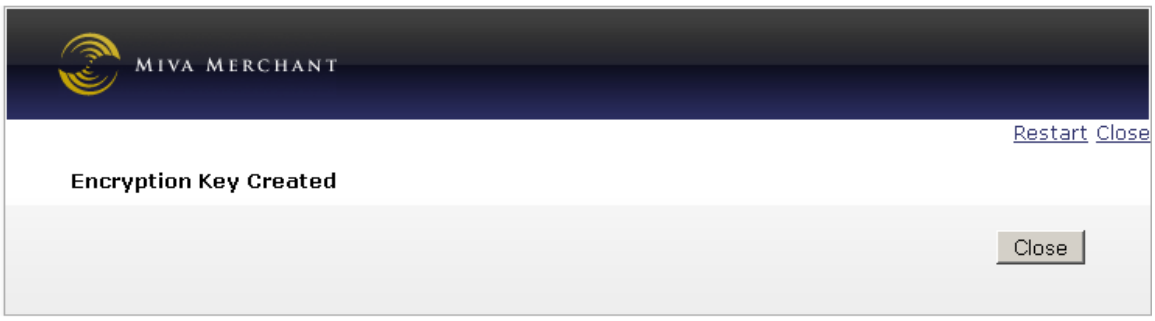


The passphrase must:

- **Be at least 16 characters long.**
- **Contain at least 1 non-numeric character, such as a punctuation mark.**
- **Contain at least 1 letter or number.**
- **Not be the same as the Prompt.**

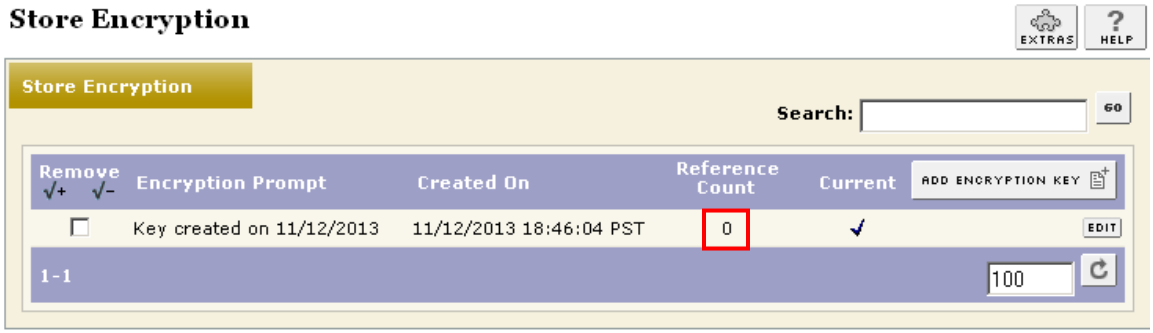
Enter your passphrase and click Next.

Click Next to confirm creation of the key.



Click Close. Your key has been created. Encryption is now enabled in your store.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.



In the Order Encryption > Store Encryption screen, the Reference Count column tells you how many orders have been encrypted with this key.

Processing Existing Orders with the Encryption Key Wizard

Follow the steps in this section if you want to enable encryption in your store, and you have existing orders with credit card information. You'll be able to:

1. **Create a new encryption key**. Creating an encryption key enables order encryption in your store.
2. **Migrate orders**. Migrating means encrypting the payment information in existing orders with the newly created Encryption Key. Only the payment information is encrypted. The rest of the order is unchanged.

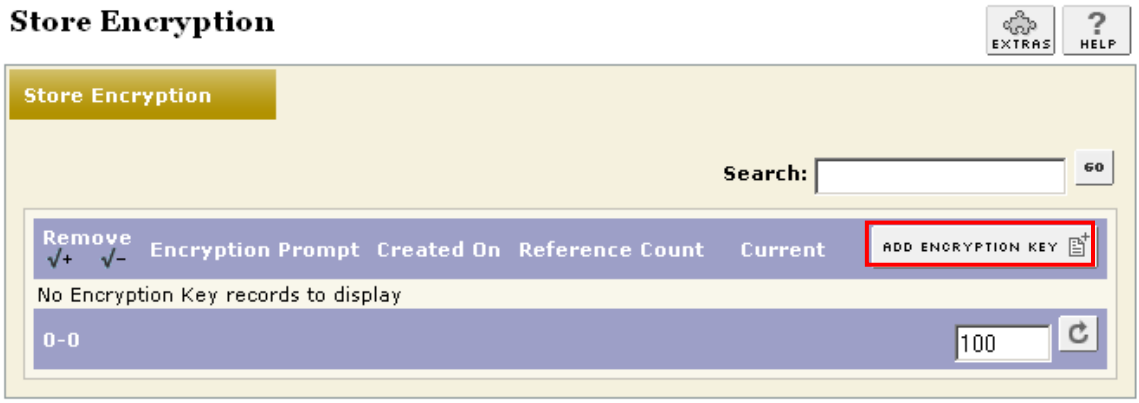
   and/or

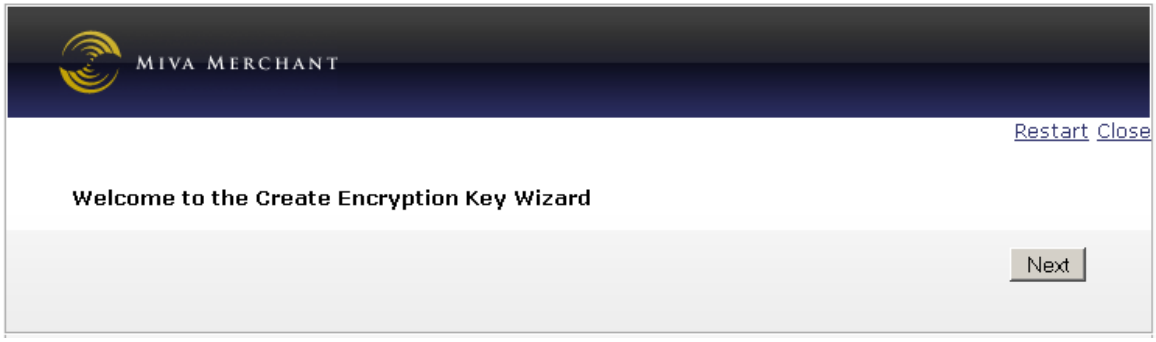
3. **Archive orders**. Archiving means deleting payment information from existing orders. The order stays in your database. Only the payment information is deleted.

To Process Existing Orders with the Encryption Key Wizard

1. Select Order Encryption from the leftnav.
2. In the Store Encryption main screen, click the **Add Encryption Key** button.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

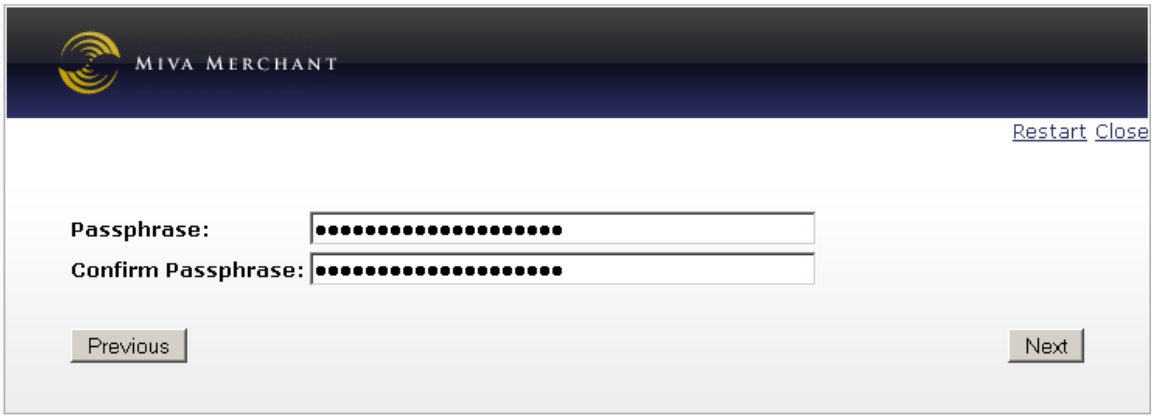




Click Next.

Enter a Prompt (a descriptive name) for the encryption key and click Next.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.



The passphrase must:

- **Be at least 16 characters long.**
- **Contain at least 1 non-numeric character, such as a punctuation mark.**
- **Contain at least 1 letter or number.**
- **Not be the same as the Prompt.**

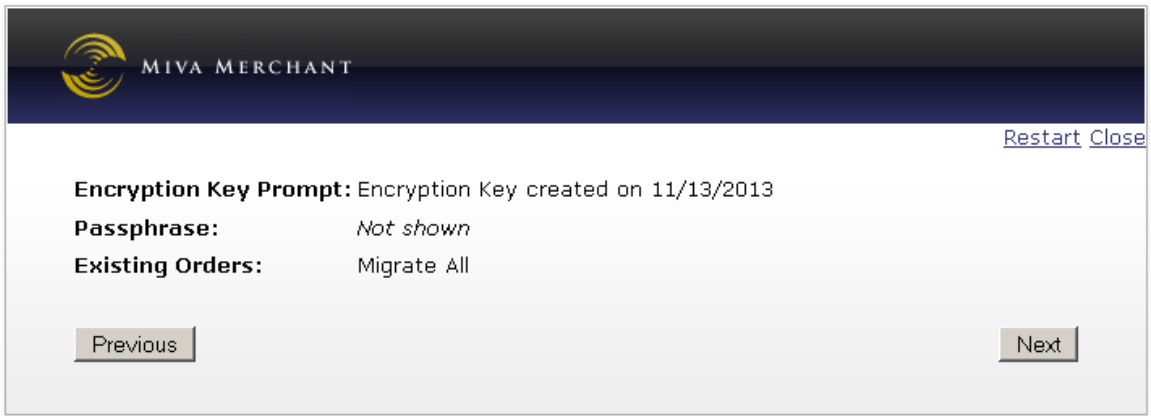
Enter your passphrase and click Next.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

In this screen you can migrate orders, archive orders, or both:

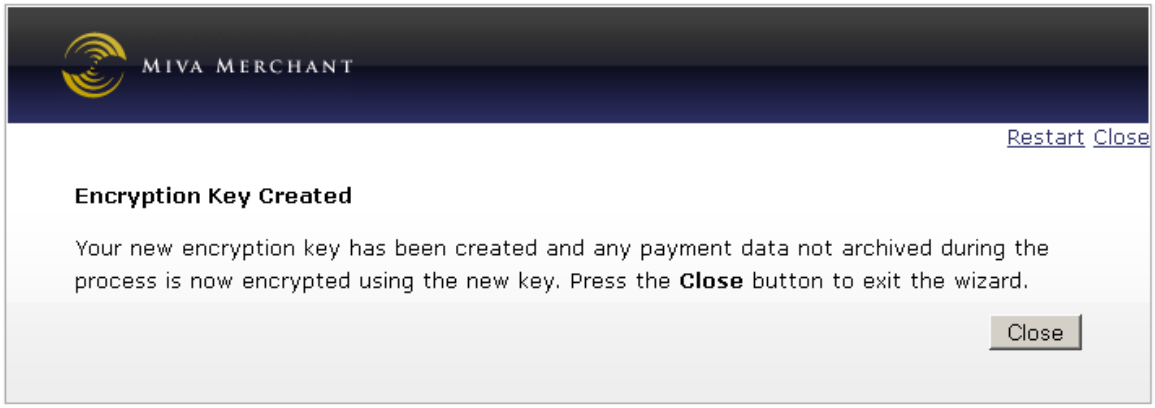
- **Migrate All: Encrypt all payment information in all existing orders.**
- **Archive Shipped:**
  - **Remove payment information from orders marked as shipped.**
  - **Encrypt payment information in all other orders.**
- **Archive All: Remove payment information from all existing orders.**
- **Archive Older Than:**
  - **Remove payment information in orders placed before the date that you select.**
  - **Encrypt payment information in all other orders.**

Select an option and click Next.



Click Next to confirm.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.



Click Close. Your encryption key has been created. The migrate/archive options that you selected have been made.

Regular Archiving in the Manage Orders Screen

The Encryption Key Wizard is usually used only once annually to enable encryption or update the Encryption Key in your store. If you'd like to Archive payment data more often than when you change your Encryption Key, you should use the Manage Orders section of the Admin.

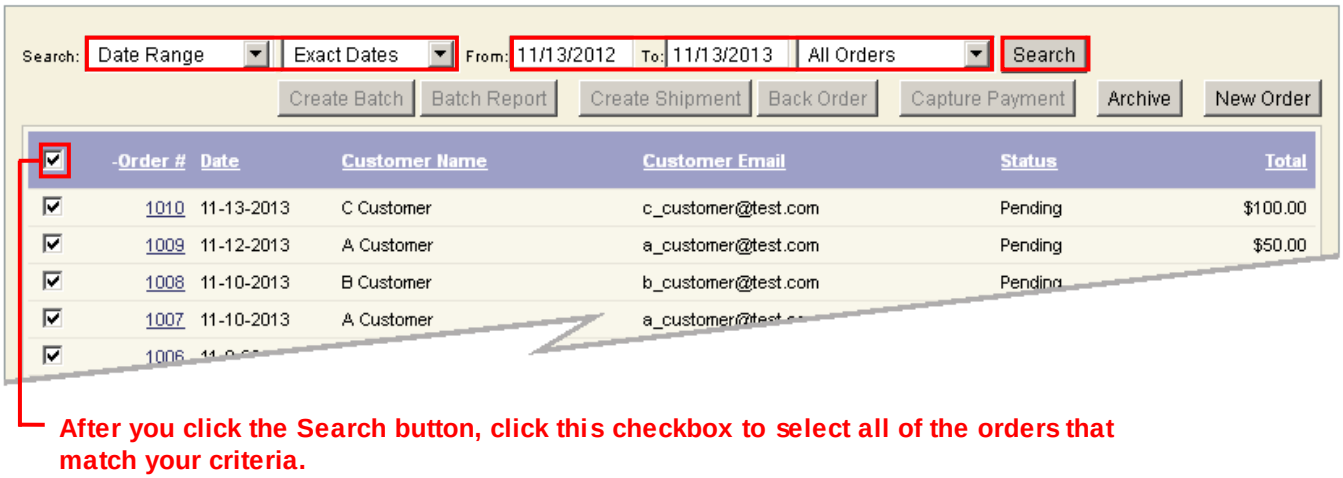
To Archive an Order

In this section we'll show you how to search for orders that are older than a given date and archive all of them.

1. Select Manage Orders from the leftnav.
2. In the Manage Orders screen:
   2.1. Select **Date Range**, **Exact Dates**, and enter **From** and **To** dates covering one year.
   2.2. Click **Search**.

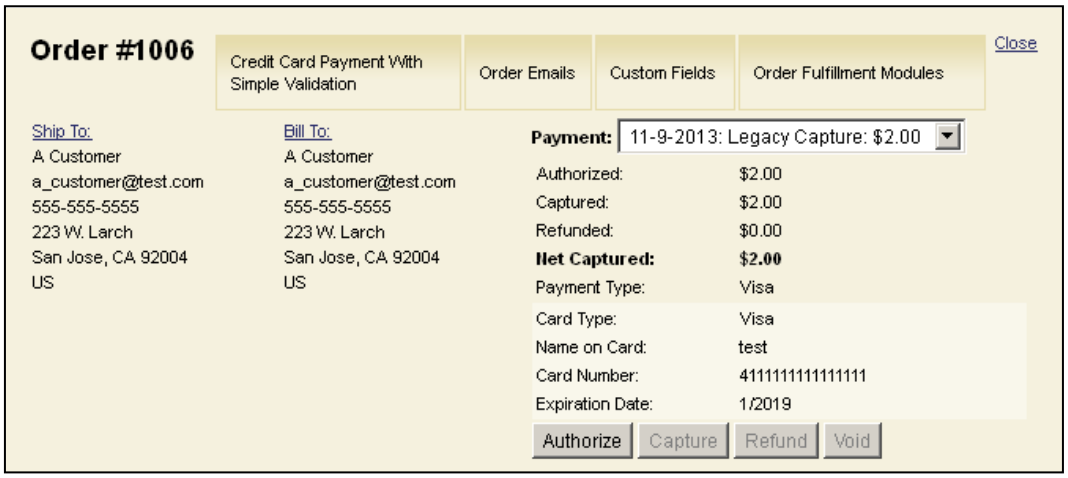
© Copyright 2005-2013, Miva Inc. All Rights Reserved.

Manage Orders



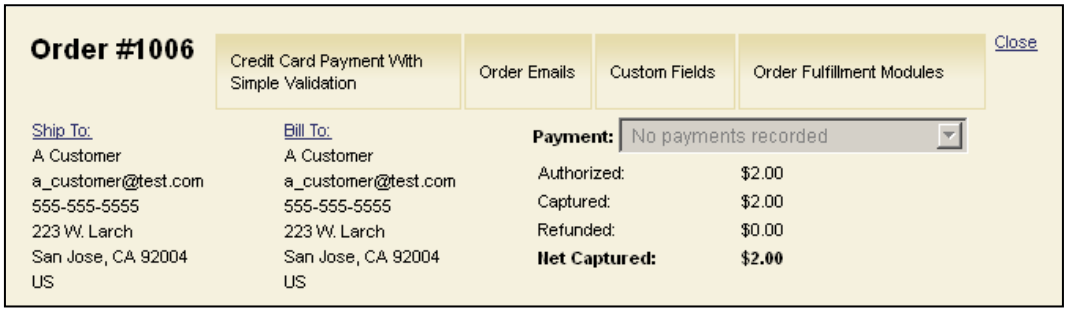
3. Click the checkbox in the title bar to select all of the orders that met your criteria, then click **Archive**.
4. A message box will appear asking you to confirm the deletion of payment information. Click **OK**.
5. Payment information has been removed from the orders that you selected.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.



Before archiving.

Note that the payment data in this example is not encrypted.



After archiving

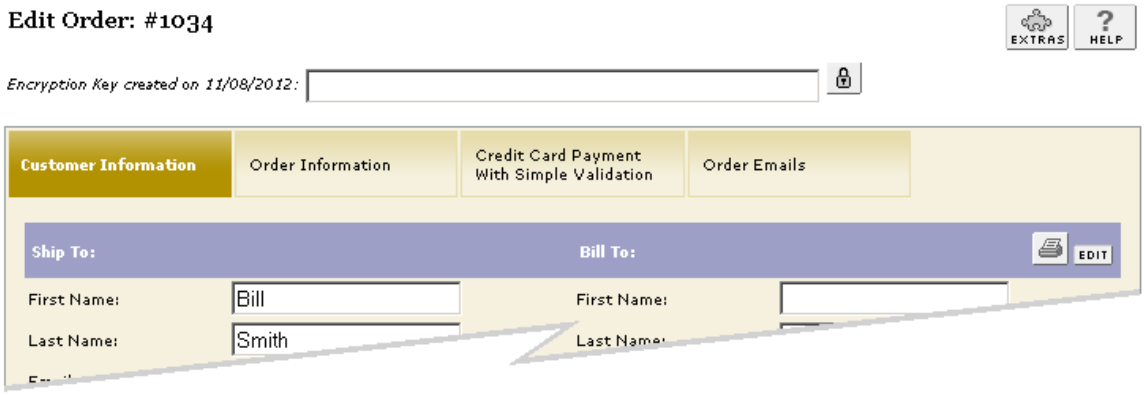
To View Encrypted Credit Card Information

If the credit card information on an order has been encrypted, you can't view the credit card data unless you know the encryption key passphrase. There are several ways to view encrypted credit card information.

In the Order Encryption Screen

1. Select Order Encryption from the leftnav.
2. In the Store Encryption screen, click the **Edit** button next to the encryption key.
3. In the Edit Encryption Key screen, select the Orders tab.
4. In the Orders tab, click the **Edit** button next to an order.
5. In the Edit Order screen, enter the passphrase and click **Update**.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.

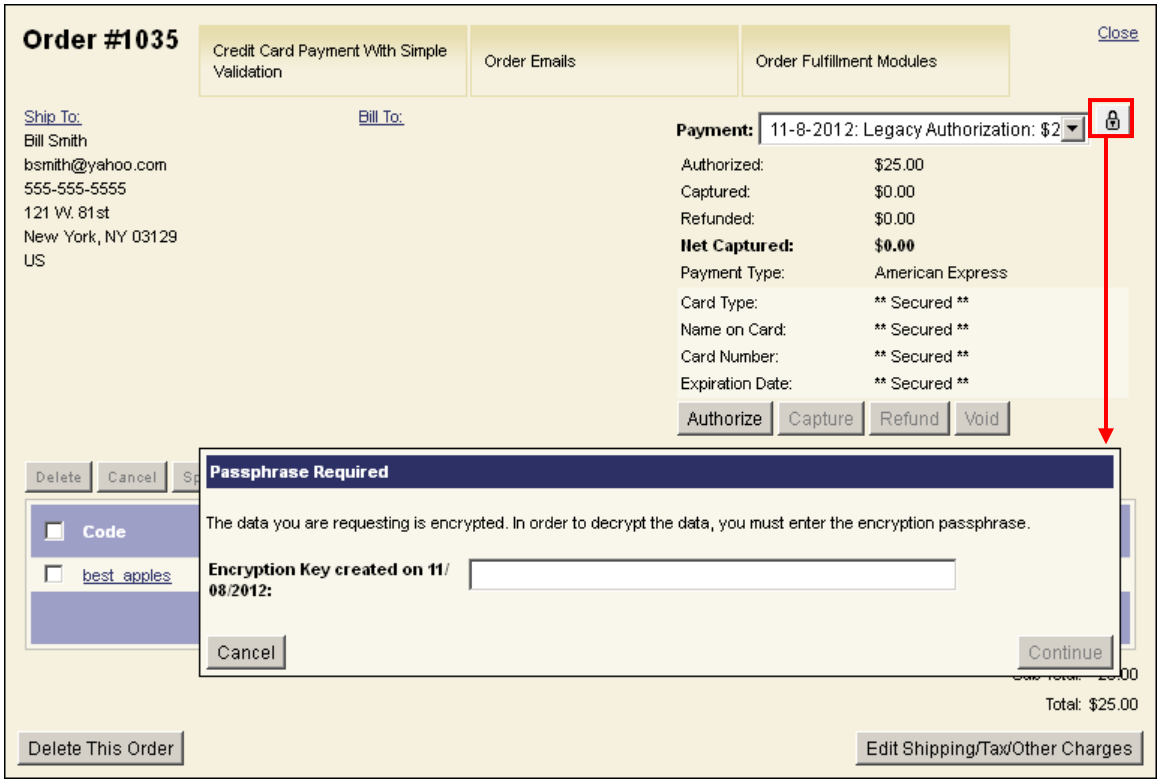


After you enter the passphrase that was used to create the encryption key and click **Update**, you'll be able to select any of the order tabs.

In the Manage Orders Screen

1. Select Manage Orders from the leftnav.
2. In the Manage Orders main screen, edit an order that has credit card information that was encrypted with the current key.
3. In the Edit Order screen, click on the lock button. Enter the passphrase and click the **Continue** button. The Edit Order screen will refresh and will openly display the credit card information.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.



In Legacy Order Processing

1. Select Utilities > Legacy Order Processing from the leftnav.
2. In the Order Processing main screen, edit an order that has encrypted credit card information.
3. In the Edit Order screen, enter the passphrase and click Update.
4. After you enter the passphrase that was used to create the encryption key, you'll be able to select any of the order tabs.

© Copyright 2005-2013, Miva Inc. All Rights Reserved.