Cybersource for Salesforce Billing Technical Guide



cybersource
A Visa Solution

Cybersource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any Cybersource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any Cybersource Service, visit the Support Center: http://www.cybersource.com/support

Copyright

©2026 Cybersource Corporation. All rights reserved. Cybersource Corporation (“Cybersource”) furnishes this document and the software described in this document under the applicable agreement between the reader of this document (“You”) and Cybersource (“Agreement""). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by Cybersource. Cybersource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, you may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of Cybersource.

Restricted Rights Legends

For Government or defense agencies: Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in Cybersource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource, Cybersource Payment Manager, Cybersource Risk Manager, Cybersource Decision Manager, and Cybersource Connect are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, and the Cybersource logo are the registered trademarks of Visa International in the United States and other countries. Bank America and the Bank America logo are the registered trademarks of Bank of America in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Confidentiality Notice

This document is furnished to you solely in your capacity as a client of Cybersource and as a participant in the Visa payments system.

By accepting this document, you acknowledge that the information contained herein (the “Information”) is confidential and subject to the confidentiality restrictions contained in Visa's operating regulations and/or other confidentiality agreements, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than its intended purpose and in your capacity as a customer of Cybersource or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non-public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non-public information would constitute a violation of applicable U.S. federal securities laws

Release: October 2026
Version: 1.7

Contents

1. Introduction 1
2. Package Installation 1
3. Configuration 1
Step 1: Assign Cybersource Permission Set 1
Step 2: Assign Cybersource Payment Gateway Page layout 2
Step 3: Add new picklist value 2
Step 4: Create Payment Gateway 3
Step 4.1: Message Level Encryption **5**
Step 4.2: Platform Events **10**
Step 4.3: Platform Cache **10**
Step 5: Configure Payment Transaction Object Page Layout 12
4. Configure the Payment Methods 13
4.1. Payment Card 13
4.2. Electronic Check Processing 13
5. Configure Features (OPTIONAL) 14
5.1. Token Management Service 14
5.2. Authorization Service 14
5.3. Capture Service 14
5.4. Refund Service 14
6. Test and Go Live 14
7. Upgrade Package 16
8. Release Notes 16

1. Introduction

- **Description:** Cybersource, a Visa solution, is the only global, modular payment management platform built on secure Visa infrastructure with the payment reach and fraud insights of a massive $500B+ global processing network. You can find out more about what Cybersource does here.
- **Categories:** Sale, Refund, Tokenization, Authorization and Capture.
- **Version:**
- **Compatibility:**

Contact

Global Partner Solutions – Customer Support: GlobalPartnerSolutionsCS@visa.com

2. Package Installation

Step 1: Install CPQ and Billing (CPQ first, then Billing) using this link:
https://install.steelbrick.com/InstallBilling

Step 2: Install the managed package from Salesforce App exchange(https://appexchange.salesforce.com/) by searching for "**Cybersource for Salesforce Billing**".

3. Configuration

Prerequisite

If you are new to Cybersource, and would like to start using Cybersource Cartridge quickly, begin by signing up for a Sandbox Account.

You will also need to create an API Key and API Shared Secret Key that you can use to authenticate requests to our sandbox server. Follow same steps to generate Production key and shared secret.

Set Field Level Security for Merchant Id, Key ID, Shared Key, Endpoint, Enable Message Level Encryption, REST Certificate, Max Wait Time (Seconds), Level of Data, Token Type fields of **Payment Gateway** (blng__PaymentGateway__c) object.

Step 1: Assign Cybersource Permission Set

The package comes with two permission sets

1. Cybersource Admin User

Assign this permission set to Admin user who would be managing the key management of Cybersource managed package. This permission set will provide read and edit access to Merchant Id, Key_Id(API Name - cybsbilling__Kyid_value__c), Shared_Key(API Name - cybsbilling__Sk_value__c), Endpoint, Enable Message Level Encryption, REST Certificate, Max Wait Time (Seconds), Level of Data, Token_Type (API Name

cybsbilling__Tk_Type__c) fields of **Payment Gateway** (blng__PaymentGateway__c) object.

2. **Cybersource Billing User**

   Assign this permission to all the users who would be doing payment processing. This permission set will provide read access to Merchant Id, Key_Id(API Name - cybsbilling__Kyid_value__c), Shared_Key(API Name - cybsbilling__Sk_value__c), Endpoint, Enable Message Level Encryption, REST Certificate, Max Wait Time (Seconds), Level of Data, Token_Type (API Name - cybsbilling__Tk_Type__c) fields of **Payment Gateway** (blng__PaymentGateway__c) object.

Step 2: Assign Cybersource Payment Gateway Page layout

The package comes with **Cybersource Gateway Layout** of Payment Gateway object (blng__PaymentGateway__c). Assign this layout to user's profile that manages the Cybersource key management.

1. Go to **Setup** by clicking the gear on the right-side top.
2. Click **Object Manager** and go to **Payment Gateway** (blng__PaymentGateway__c) object detail.
3. Click **Page Layouts**.
4. Click **Page Layout Assignment**.
5. Click **Edit Assignment** to assign the **Cybersource Gateway Layout** to appropriate profile.

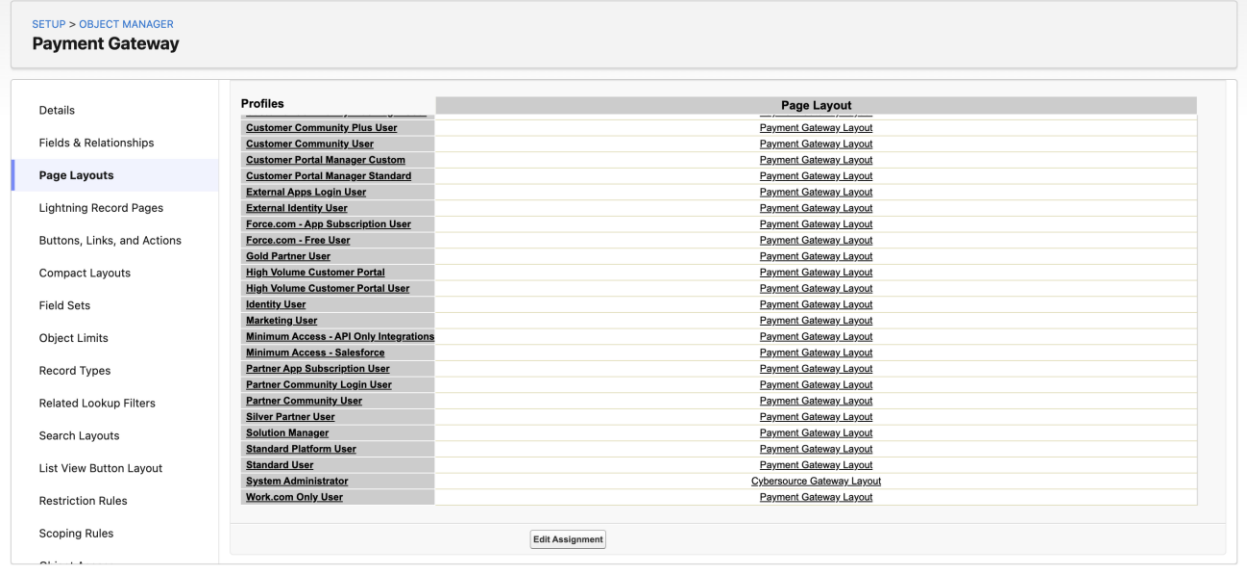


Fig 1: Cybersource Payment Gateway Page Layout

Step 3: Add new picklist value

1. Go to **Setup** by clicking the gear on the right-side top.
2. Click **Object Manager** and go to **Payment Gateway** (blng__PaymentGateway__c) object detail.
3. Click **Fields and Relationships.**
4. Click **Gateway Type** (blng__GatewayType__c).

5. Click **View Gateway Type Value Set** under **Values** section.
6. Click **New** under **Values**.
7. Enter "**Cybersource Payments"** and click **Save**.

Step 4: Create Payment Gateway

1. Click on **App Launcher > Payment Gateways. (bIng__PaymentGateway__c)**
2. Click **New**.
3. Enter the required details

Fields	***Description***	***Value to Set***
Payment Gateway Name	Enter Payment Gateway name.	
Merchant ID	Cybersource Merchant ID.	
Gateway Type	Select the Payment Gateway Type.	**Cybersource Payments**
Endpoint	Select Test (Test) or Production (Production)	
Active	Select the checkbox.	
Default	Select the checkbox	
Developer ID	Unique identifier generated by Cybersource for System Integrator.	
Key_Id	Cybersource REST KeyId. Follow link for directions.	
Level of Data	Select the required Level of Data from the picklist. Required only for Credit Card payments.	
Token_Type	Select the required Token Type from the picklist.	
Shared_Key	Cybersource REST Secret Key	

Table 1: Payment Gateway Settings

NOTE*:*

- The default value for token type is 'Payment Instrument ID'. The user can change the value as needed. Token type is a one-time choice and cannot be changed once the first token request has been called.
- Merchants migrating from the Native Salesforce solution to Cybersource will have their Payment token stored as Customer ID tokens.

L2/L3 Data Processing

1. The TAA fields in Order layout are required whenever the card type is American Express. It can be added while creating an order by following the steps below.
   - Click on **App Launcher > Orders(Order)**
   - Click **New**.

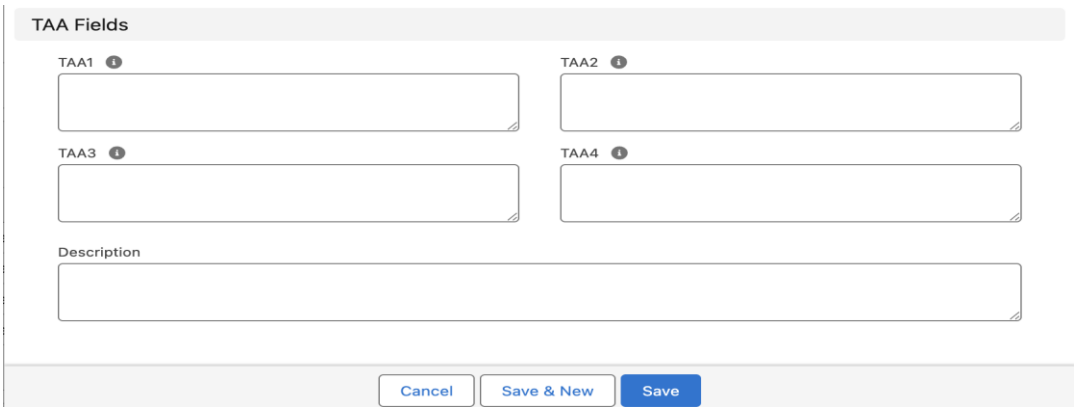


Fig 2: TAA Details Section in Order Page Layout

2. The VAT Registration Number field is added in the Billing Account page layout and User Page Layout which is required by few processors.

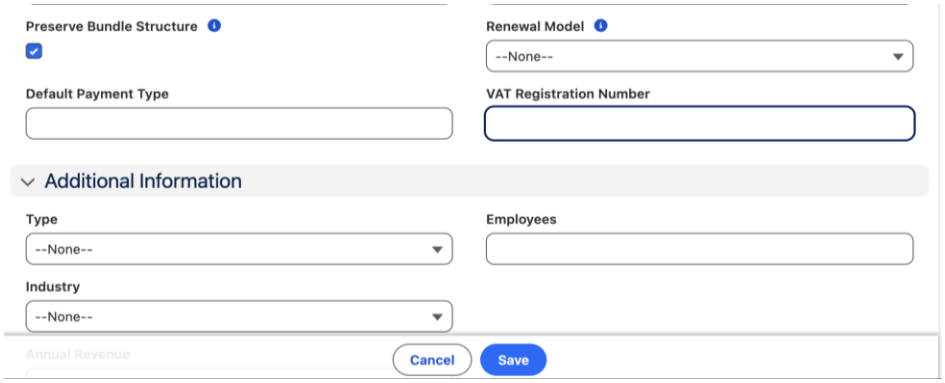


Fig 3: Billing Account Page Layout



Fig 4: User Page Layout

Step 4.1: Message Level Encryption

Message Level Encryption (MLE) uses certificates that ensure each message is securely encrypted and tied to the sender's verified identity, without needing to share secret keys in advance. This provides stronger authentication, easier key management, and better protection against fraud or tampering.

A shared secret uses the same key for both sending and receiving messages, meaning both parties must securely exchange and protect that key in advance. While it can be simpler, it offers less identity verification and can be more vulnerable if the key is compromised.

To support Message Level Encryption,

1. Upload the p12 certificate as a Static resource.
   a. Follow the steps mentioned in this link to generate a p12 Certificate in the Business Center.
   b. Note down the password set for the p12 key.
   c. Download the generated p12 file.
   d. Convert the p12 file to .pem format in OpenSSL using the below command **Command: openssl pkcs12 –in test.p12 -cacerts –nokeys –out cert.pem** In the above command replace <test> with your p12 file name
   e. Upload the generated p12 in static resource
      i. Click **Setup**
      ii. In the quick find box,enter **static resource** Click on **New** button
      iii. Enter a unique name and upload the above generated file
      iv. Click **Save**
2. Configure the "**bIng__PaymentGateway__c"** page layout and verify if all the fields are available in the Payment Gateway Detail.

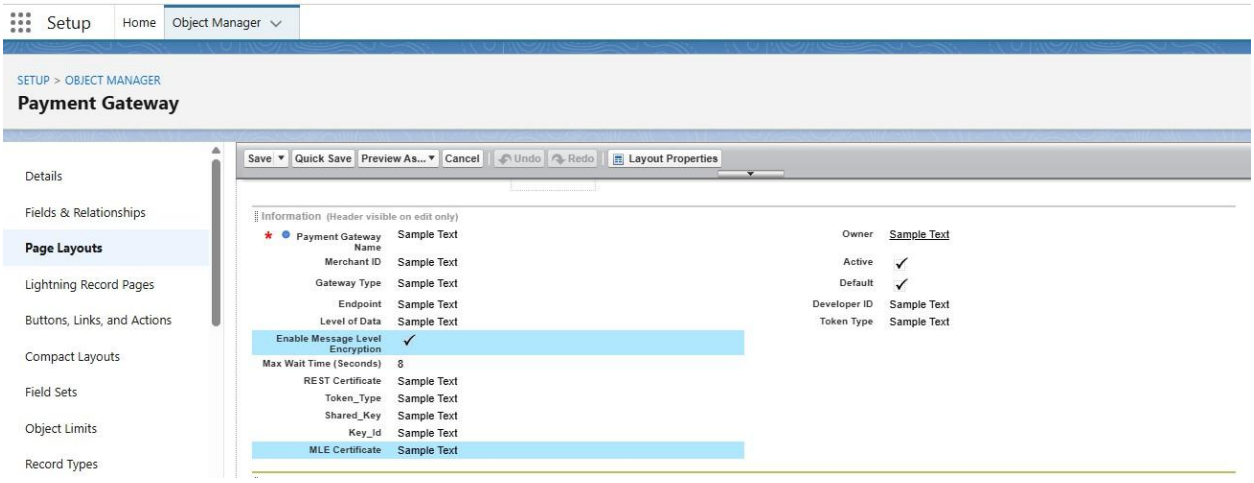


Fig 5: Payment Gateway Page Layout

3. If the REST Certificate field is visible on the Lightning Record Page, edit the blng__PaymentGateway__c Lightning Record Page as shown in the diagram below. Set the UI Behaviour to None, remove the REST Certificate field, and then save and activate the Lightning Record Page to apply the changes.

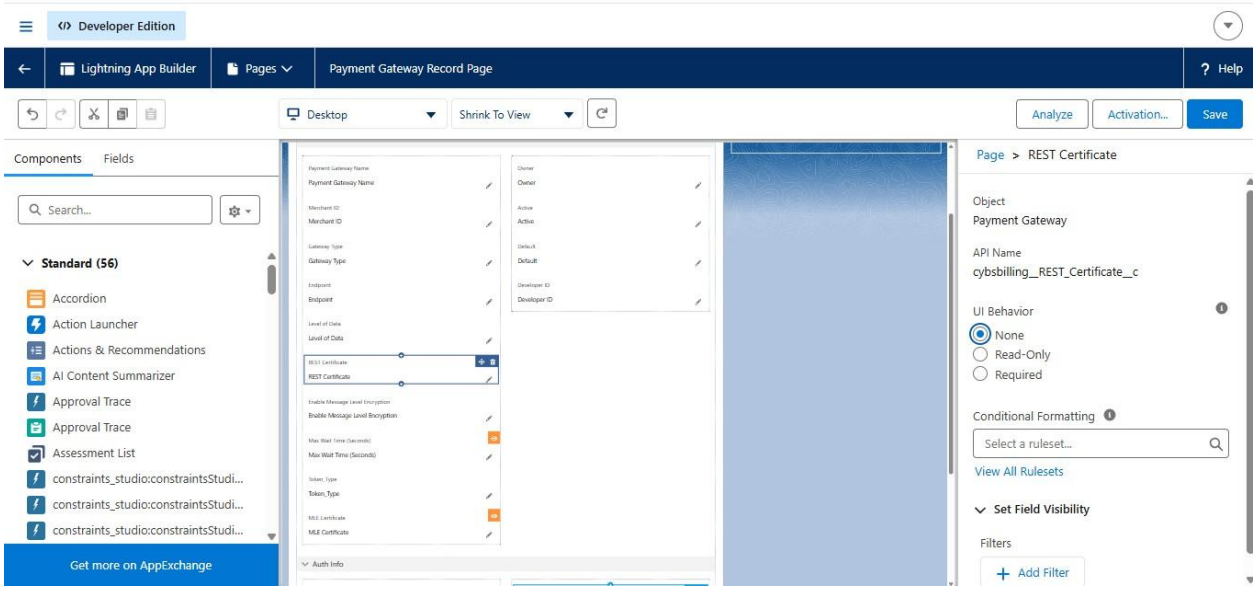


Fig 6: Payment Gateway Lightning Record page

4. Ensure all the fields are available & set the **"MLE Certificate"** field property as **"None"** in the lightning record page and Check filter Enable Message Level Encryption equal to 'TRUE'.

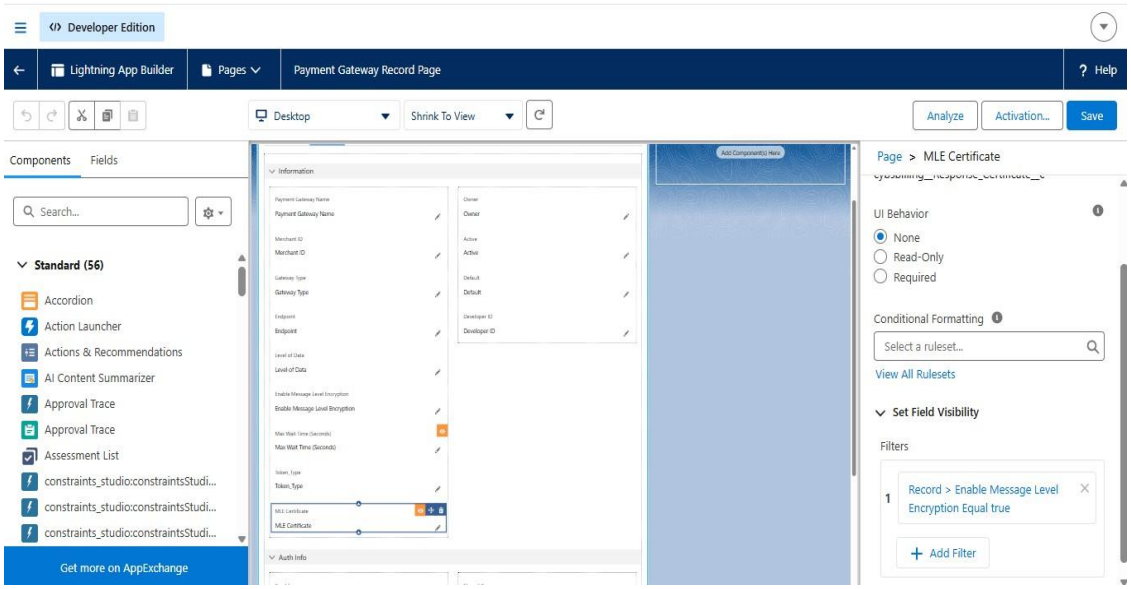


Fig 7: Payment Gateway Lightning Record page

5. Save the lightning record page.
6. Activate the lightning record and Assign as Org Default

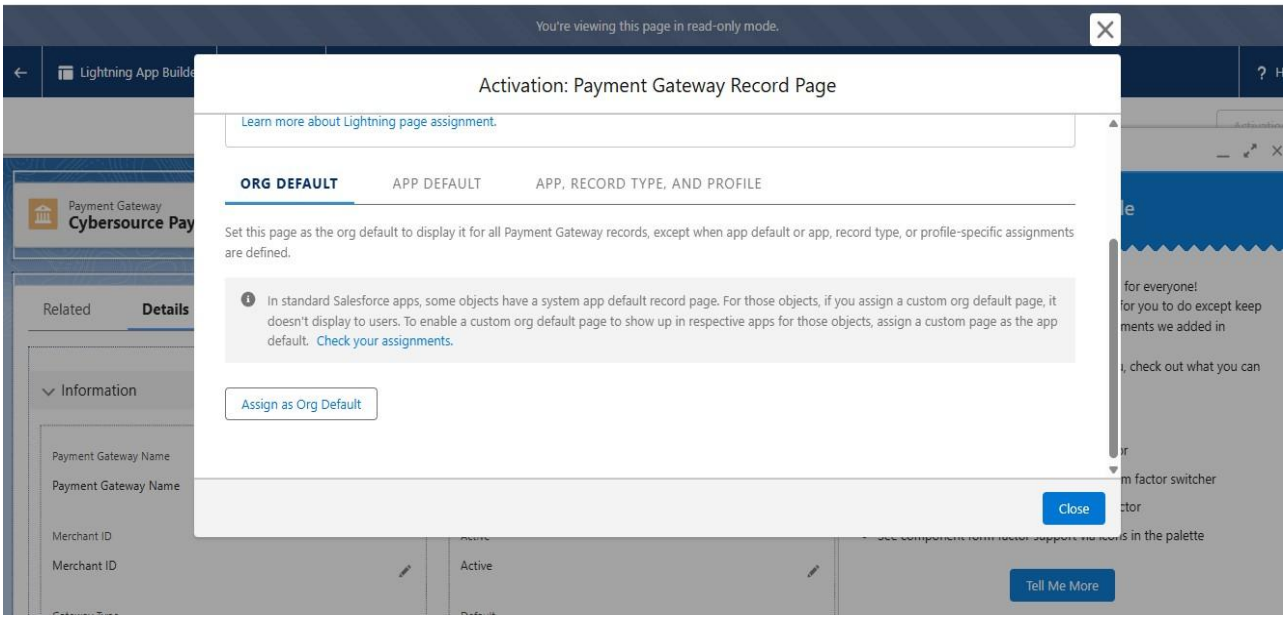


Fig 8: Payment Gateway Lightning Record page Activation

7. Check the **"Enable Message Level Encryption"** checkbox by navigating to the Payment Gateway created in step 4 to support Message Level Encryption, and in the **"MLE Certificate"** field, enter the name of the static resource created while uploading the p12 certificate.
8. **Max wait time** is the duration needed to encrypt the payload before sending it to Cybersource. If this time limit is exceeded, the transaction will fail, and an error message 'Missing encrypted payload' is displayed during the payment process. It is recommended to increase the wait time by 1-second increments until the payload is successfully encrypted.

Fields	***Description***	***Value to Set***
Enable Message Level Encryption	Level Select the checkbox to enable Message Encryption.	
MLE Certificate	Enter the Static resource name created while uploading the p12 Certificate.	
Max Wait Time (Seconds)	A default value is 2s, can also be adjusted in case required.	

Table 4.1: Payment Gateway Settings Continued

9. Go to **Account -> open a record** -> Click on "**Edit Page**"

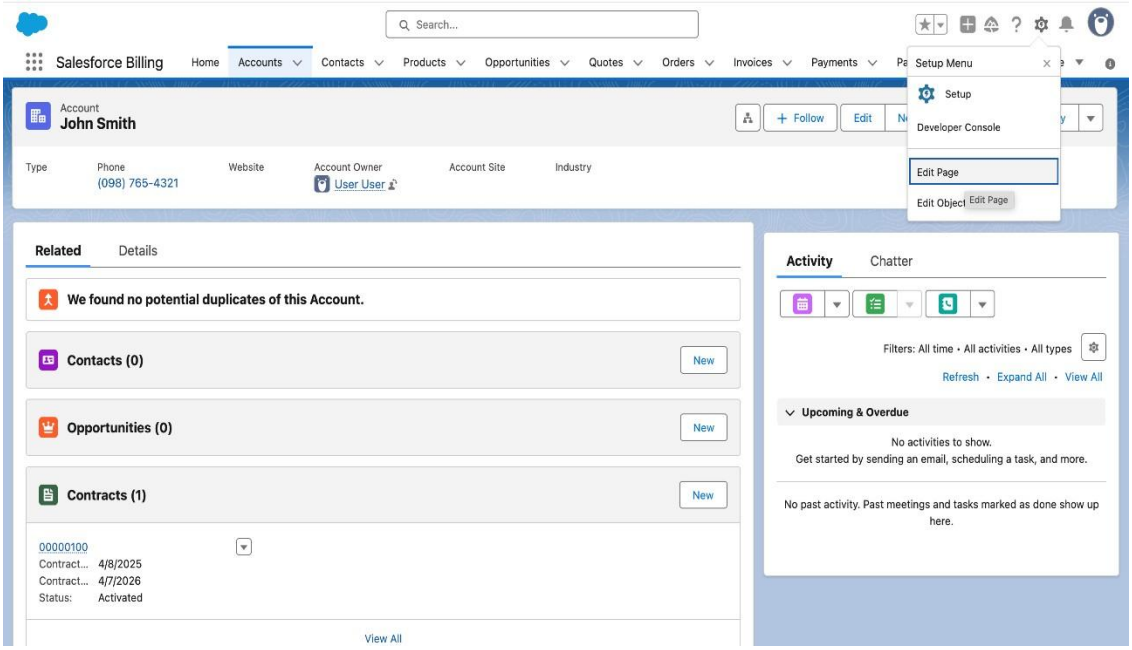


Fig 9: Account Record page

10. Edit the Account object lightning record page, drag the custom Lightning Web component **"PTS_EncryptComponent"** and drop it inside the Activity tab.

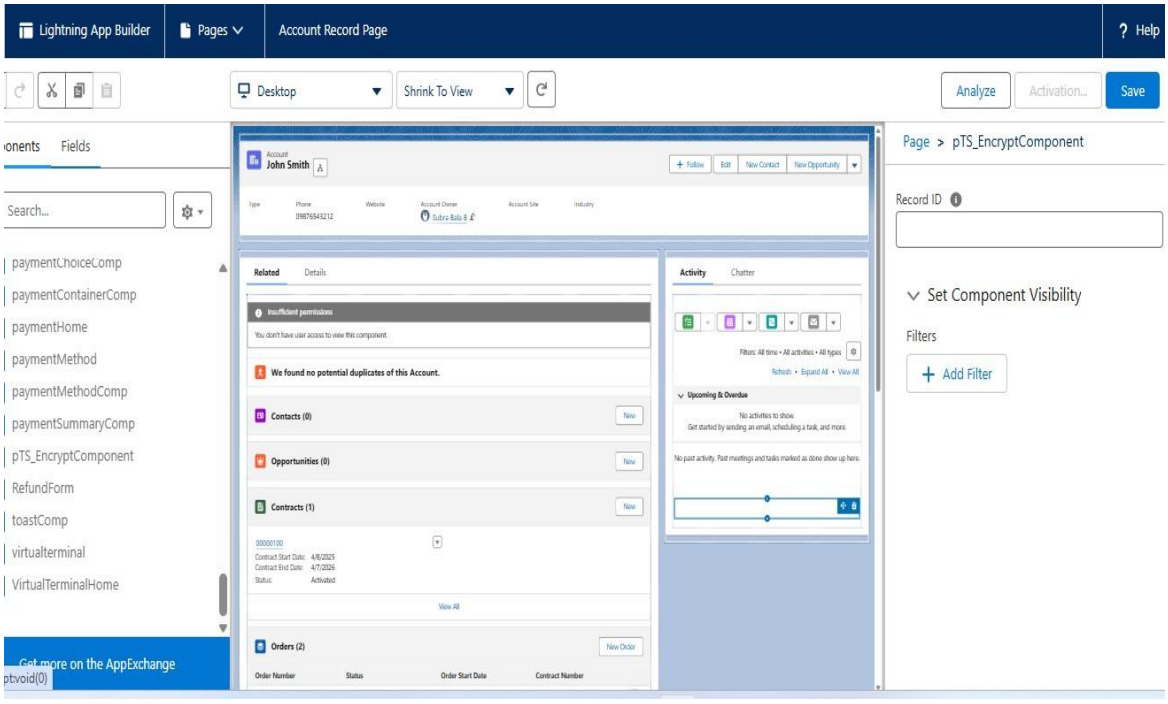


Fig 10: Account Lightning Record page

11. Save the changes and activate the page, Assigning it as Org Default.

12. Go to **Payment -> open a record ->** Click on "**Edit Page**"

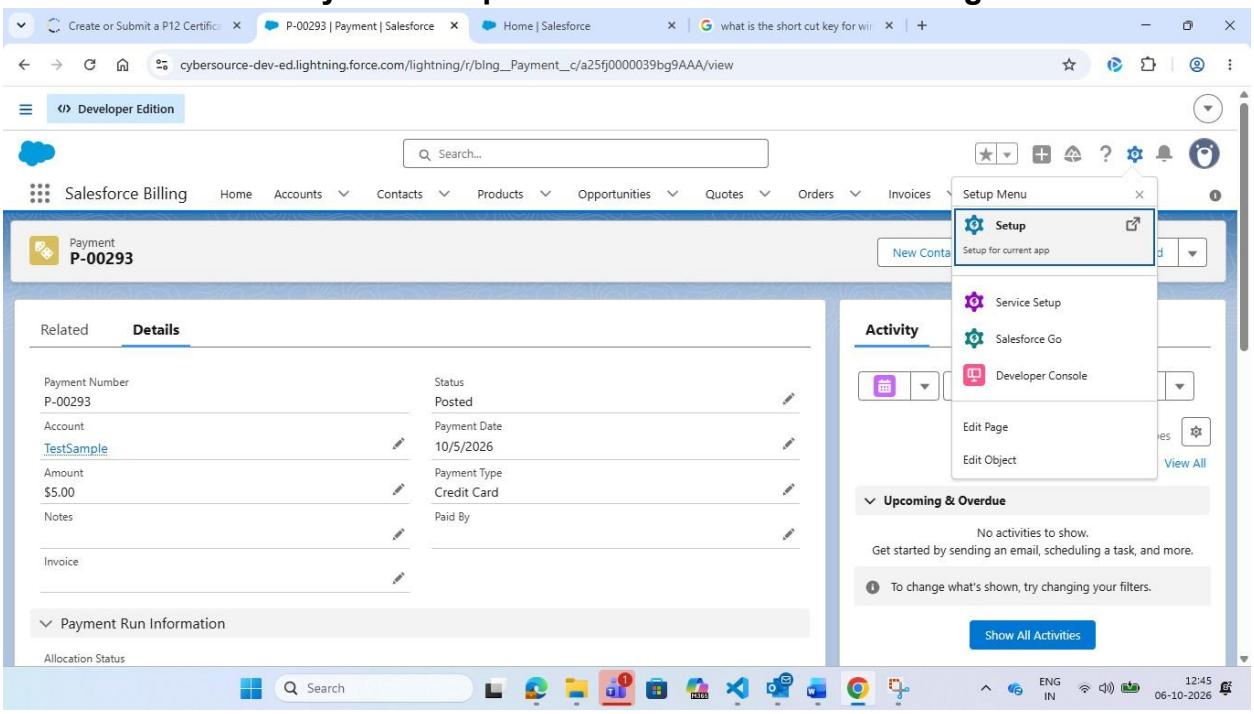


Fig 11: Payment Record page

13. Edit the Payment object lightning record page, drag the custom Lightning Web component **"orderManagementMLE"** and drop it inside the Activity tab.

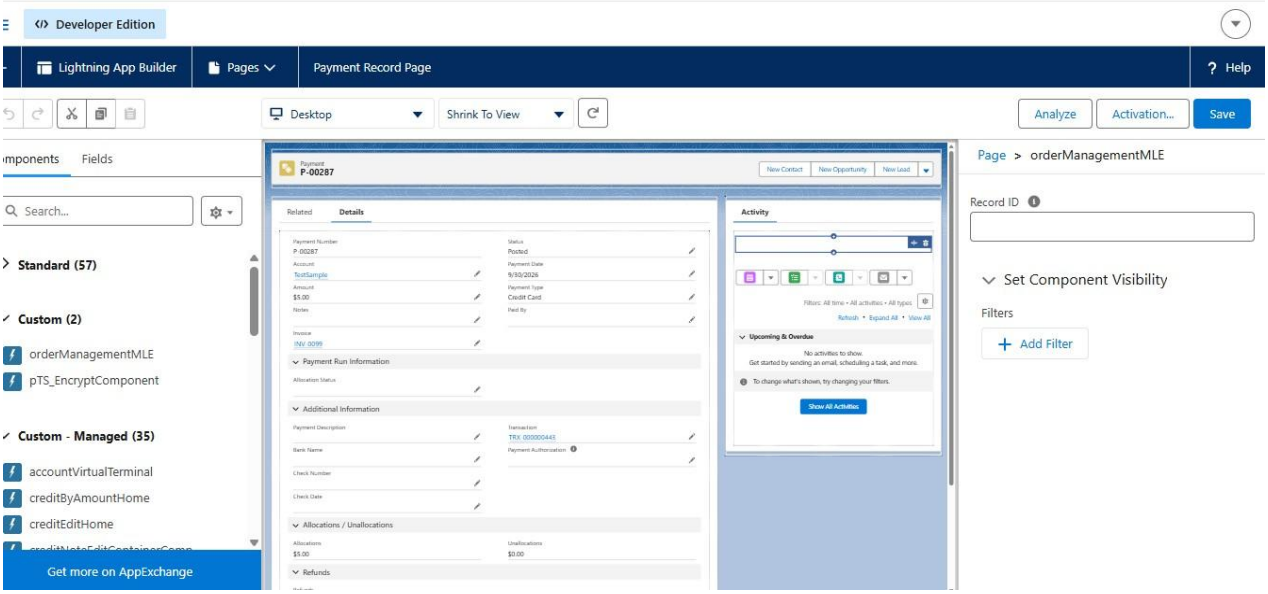


Fig 12: Payment Lightning Record page

14. Save the changes and activate the page, Assigning it as Org Default.

Note: • If a plain-text request is sent instead of an encrypted request, increase the Max Wait Time (Seconds) setting to avoid potential timeout issues.

Step 4.2: Platform Events

Ensure that platform events have been created with the Channel Names as ‘Charge Transaction MLE’ and ‘Decrypt Payload’

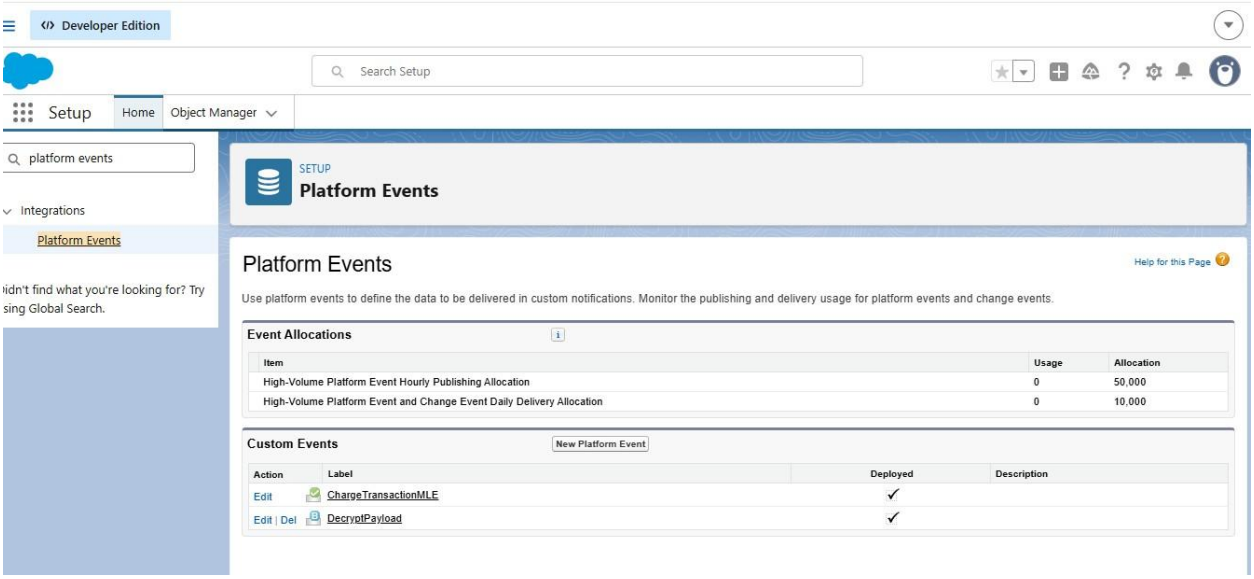


Fig 13: Platform Events

Step 4.3: Platform Cache

Ensure that a Platform Cache partition has been created with Partition Name as ‘AccessToken’ and ‘AllowedCapacity’ value as 3.

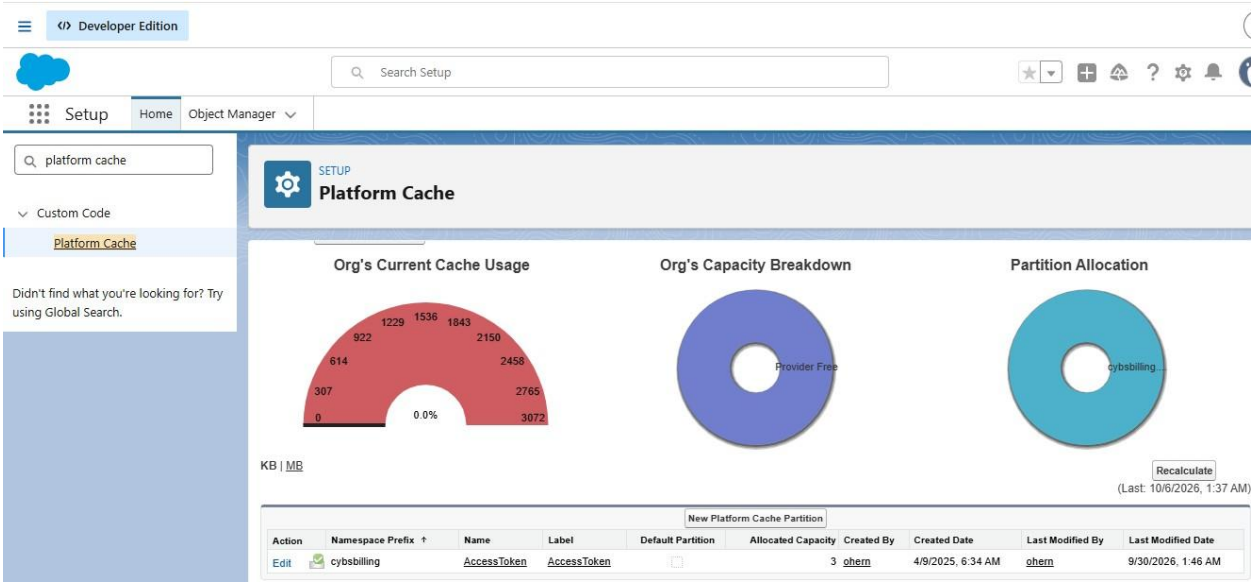


Fig 14: Platform Cache

If the platform cache does not exist, create new platform cache. Create Platform Cache by following Steps:

i. Click setup
ii. In the quick find box enter platform cache
iii. Create New
iv. Set the Label as ‘AccessToken’
v. Allocate Session cache 1 and Org cache 2

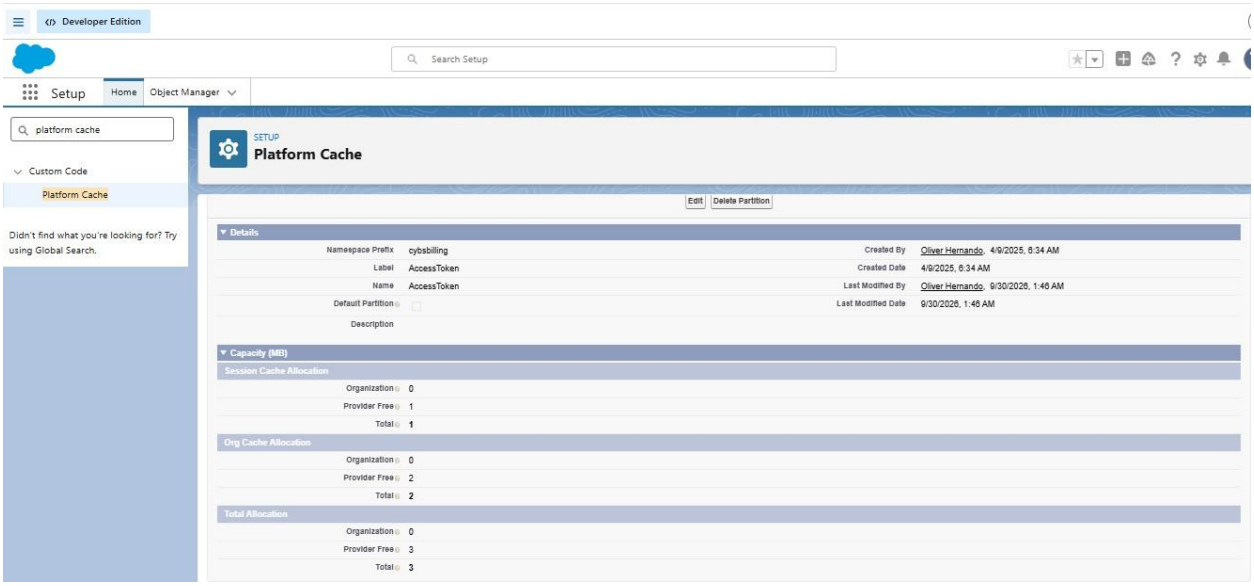


Fig 15: Platform Cache

Step 5: Configure Payment Transaction Object Page Layout

1. The payment transaction page layout must contain the following fields.
    a. Active Profile
    b. Authorization Code
    c. Calculated Risk Score for Order
    d. Card Scheme
    e. Commercial Card
    f. Cybersource Merchant ID
    g. Eligible for Level III
    h. Merchant Reference Number
    i. Payment Card Bin
    j. Payment Card Token ID
    k. Pre-Auth Decision
    l. Profile Action
    m. Profile Selector Rule
    n. Reason Code
    o. Reconciliation ID
    p. Scheme Reference ID

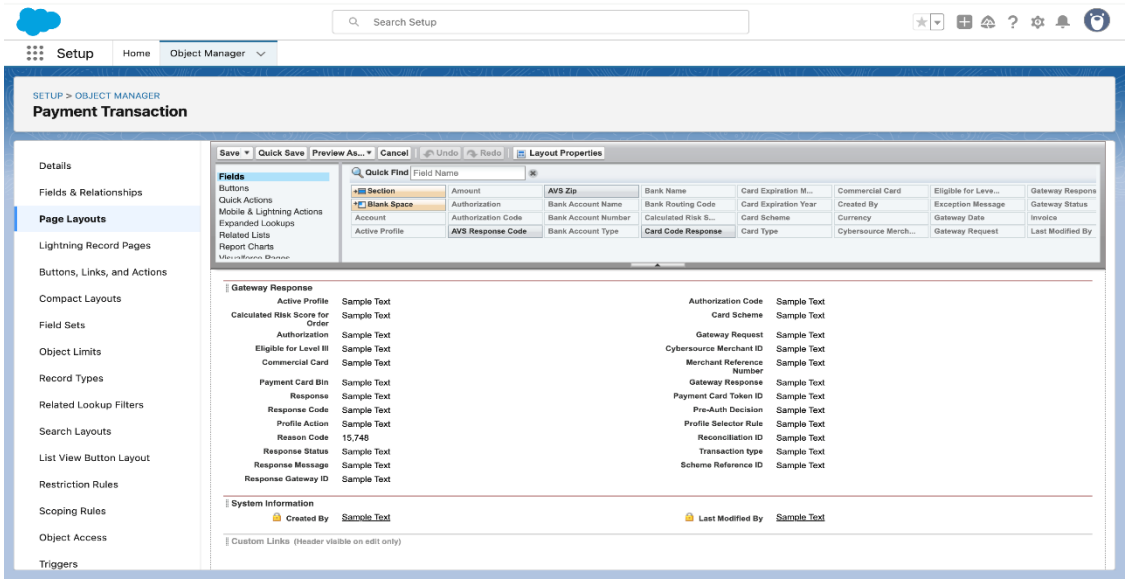


Fig 14: Payment Transaction Page Layout

2. Ensure that the payment transaction object consists of the below lightning record page and is activated.

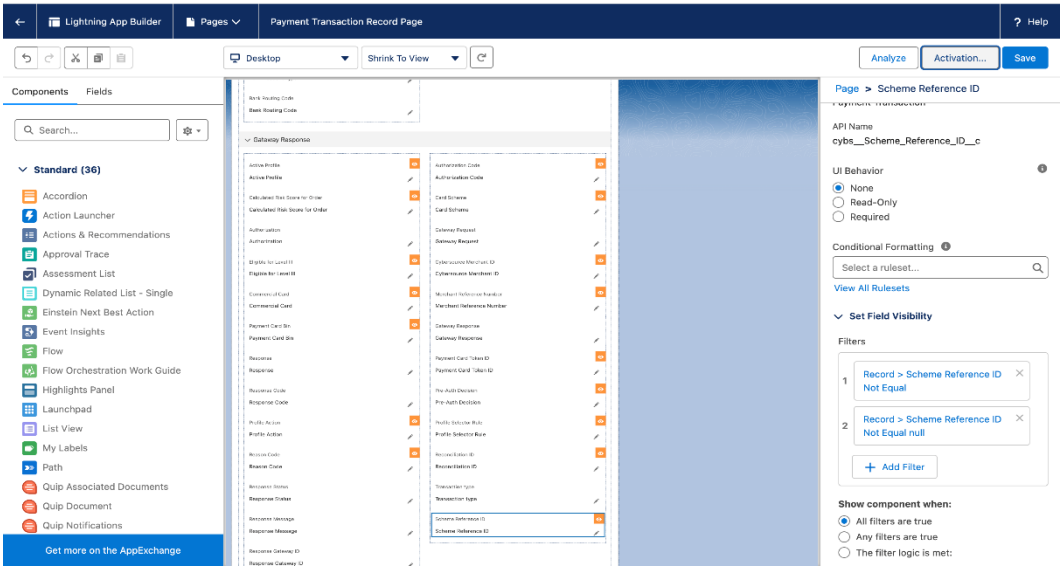


Fig 15: Payment Transaction Lightning Record Page

4. Configure the Payment Methods

4.1. Payment Card

All payments through the Cybersource cartridge will be processed as a authorize and capture request(sale) in a single message. Therefore, you will not need to capture transactions afterwards. See Section 5.2 if you want to authorize only and capture through another means.

Package supports Visa, Master Card, American Express and Discover cards by default. Create custom metadata type “CardType” records to support other card types. Follow below steps:

1. Goto **Setup**.
2. Search for custom metadata type from quick find.
3. Click on **“Manage Records”** against **“CardType”** metadata type.
4. Click on **“New”** button.
5. Enter following data
    a. **Label:** <card type>
    b. **CardType** Name field will be auto-populated.
    c. **Value:** Look for corresponding value from link.

4.2. Electronic Check Processing

Cybersource Billing package supports ACH payment. There are no explicit configurations required to process ACH payments.

5. Configure Features (OPTIONAL)

5.1. Token Management Service

Refer to this link to learn about Cybersource's Token Management service. Cybersource Billing package supports only for Card payments and not for ACH payments.

5.2. Authorization Service

All payments through the Cybersource cartridge will be processed as a authorize and capture request (sale) in a single message. If you want to process authorize only, you can make use of this exposed method.

```
Map<String, blng.TransactionResult> obj =
PTS_BillingPaymentAdapter.processPayments(blng.TransactionParameter>
mapOfTransactionParameterById, blng.PaymentGatewayParameter
paymentGatewayParameter);
```

TransactionType of blng.PaymentGatewayParameter should be "**authorizeTransaction**" to process authorization service. Refer to this link to learn about blng.TransactionParameter class.

5.3. Capture Service

All payments through the Cybersource cartridge will be processed as a authorize and capture request (sale) in a single message. If you have used the Authorization Service method to only authorize payments, you can make use of this exposed method for capturing the authorization.

```
Map<String, blng.TransactionResult> obj =
PTS_BillingPaymentAdapter.processPayments(blng.TransactionParameter>
mapOfTransactionParameterById, blng.PaymentGatewayParameter
paymentGatewayParameter);
```

TransactionType of blng.PaymentGatewayParameter should be "**captureTransaction**" to process authorization service. Refer url to know more about blng.TransactionParameter class.

5.4. Refund Service

Cybersource Billing package supports Credit Card refunds electronic refunds. Refer to this link to know how salesforce Billing processes Refund.

6. Test and Go Live

Before you start accepting payments, test your integration in Test sandbox:

The sandbox simulates the live payment gateway. The sandbox never processes an actual payment. We do not submit sandbox transactions to financial institutions for processing. The sandbox environment is separate from the live production environment, and it requires separate credentials. If you use your production credentials in the sandbox or vice versa, you get a 401 HTTP error.

Test your integration, and configure your live account, so you can start processing live transactions.

Ready to Go Live

1. Install the managed packaged in Production Org.
2. Assign Cybersource Permission set in Production Org by following Step link.
3. Assign Cybersource Payment Gateway page layout in Production Org by following steps in link.
4. Add a new picklist value **"Cybersource Payments"** to **"Gateway Type"** field of **"Payment Gateway"** object by following steps in link. Make sure picklist value is "**Cybersource Payments**".
5. Create a new Payment Gateway record in your Production Org by following steps in link. Make sure Endpoint is selected "Production".

Troubleshoot:

Issue: Script-thrown exception (System Code) - No implementation registered for service interface Cybersource Payments.

Solution:

1. Navigate to Setup → Custom Settings → Payment Gateway Config → Manage.
2. Click Cybersource Payments. Edit Gateway Class Name if an incorrect cybsbillinbillling namespcae is identified.
3. Update or remove the additional billing text and save the record.



Fig 16: Payment Gateway Configuration Detail

7. Upgrade Package

Follow the standard Salesforce process to upgrade the “Cybersource for Salesforce Billing” package. Please refer to this link for more details.

8. Release Notes

Version 1.7.0 (October 2026)

- Added Response MLE support
- JWT Authentication migration
- Added Message level encryption support for OM Services

Version 1.6.0 (May 2026)

- Supports Payments using Payment Schedulers
- Fixed a SOQL query issue related to BillingCompany field retrieval

Version 1.5.0 (April 2025)

- Added Message Level Encryption Support

Version 1.4.0 (October 2024)

- L2/L3 Data Processing
- Token type support for Tokenization

Version 1.3.0 (June 2024)

- HTTP header updates
- Amex card bug fix

Version 1.0.0 (July 19, 2021)

- Add Sale & Refund services for Card Payment method.
- Added API services for Authorization & Capture.
- Supports Card tokenization.
- Added Refund service for PayPal payment method.
- Supports eCheck payment method.