

Cybersource Payments for Salesforce B2B and D2C - Technical Guide



cybersource
A Visa Solution

© 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 Unpublished rights reserved under the copyright laws of the United States.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 and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource and Cybersource Decision Manager are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, the Cybersource logo, and 3-D Secure are the registered trademarks of Visa International 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.

Contents

- Introduction.....4**
- Supported Features.....5**
- Supported Versions.....6**
- Prerequisites..... 7**
- Release Notes..... 8**
- Installation.....10**
- Configuration..... 11**
- Payer Authentication..... 15**
- Tokenization.....17**
- Message Level Encryption.....18**
- Platform Cache.....20**
- Checkout Page..... 21**
- Order Management.....22**
- Support & Troubleshooting.....23**
- Upgrade.....24**

Introduction

Overview of the Cybersource Payments App for Salesforce B2B Commerce and D2C Commerce.

The Cybersource Payments App for Salesforce B2B Commerce and D2C Commerce allows merchants to connect their Salesforce B2B or D2C store to Cybersource for payment processing.

Supported Features

List of features supported by the Cybersource Payments App for Salesforce.

Available Features

- Credit/Debit Cards
- Payer Authentication / 3-D Secure
- Tokenization

Supported Versions

Salesforce platform versions supported by the Payments App.

Compatible Platforms

Our app works with the following:

- Salesforce B2B Commerce (Aura and LWR)
- Salesforce D2C Commerce (LWR only)
- Salesforce Order Management Lite

Prerequisites

Requirements for installing and using the Cybersource Payments App.

Salesforce Requirements

A Salesforce B2B Commerce license (legacy), Salesforce Commerce Cloud Growth license, or Salesforce Commerce Cloud Advanced license.

Custom Labels

The following custom labels must be created in your Salesforce Org before installing the app:

- Enter PO Number
- Placeholder Enter PO Number
- Placeholder PO Billing Address
- PO Billing Address

The category for each custom label is PO Payment

Cybersource Requirements

- Cybersource transacting Merchant ID
- REST Shared Secret. See [here](#) for details

Optional

The following Cybersource products are optional but need to be enabled for your Merchant ID if you want to use them:

- Payer Authentication for 3-D Secure
- Tokenization

Release Notes

Version history and feature updates for the Cybersource Payments App.

Version 1.8.0

- Fixed issue where D2C Payment Component was greyed out

Version 1.7.0

- Microform Sub Resource Integrity
- D2C Commerce support (LWR only)
- B2B Commerce LWR support
- Order Management Lite support
- Cybersource Token Management Service (TMS) support

Version 1.6.0

- Replace Microform v0.11 with v2
- Salesforce API version update

Version 1.5.0

- Cybersource Message Level Encryption support

Version 1.4.0

- Purchase Order payment support

Version 1.3.0

Initial release supporting:

- Credit/debit card payments
- Microform for secure card capture
- Payer Authentication / 3-D Secure

Installation

How to install the Cybersource Payments App for Salesforce B2B and D2C Commerce.

To install the app, download Cybersource Payments for B2B and D2C Commerce from the Salesforce App Exchange.

1. Navigate to the Salesforce App Exchange.
2. Search for "Cybersource Payments for B2B and D2C Commerce".
3. Download and install the app to your Salesforce organization.

The Cybersource Payments App will be installed in your Salesforce organization and ready for configuration.

Configuration

Complete configuration steps for the Cybersource Payments App including payment gateway setup, trusted sites, and payment configuration.

After installation, several configuration steps are required to set up the Cybersource Payments App.

1. Create a Payment Gateway Provider

Creating a Payment Gateway Provider is not supported from the Salesforce UI and needs to be done through workbench by connecting to your organization:

Endpoint to be used - (MD/ToolingAPI): </services/data/v48.0/tooling/objects/PaymentGatewayProvider>

Payload:

```
{
  "ApexAdapterId":< ID of PTS_PaymentAdapter.cls apex class>,
  "DeveloperName":"Cybersource_Provider",
  "MasterLabel":" Cybersource_Provider ",
  "IdempotencySupported":"Yes",
  "Comments":"Comments"
}
```

2. Configure Named Credential

The package comes with default named credentials:

- Payment for test transactions
- Payment_Live for production transactions

3. Create a Payment Gateway Record

a. Choose **App Launcher > Payment Gateways**

b. Choose **New**

c. Fill in the fields as follows:

Field Name	Value
Payment Gateway Name	Cybersource_Test (for test) / Cybersource_Live (for production)

Field Name	Value
Payment Gateway Provider	As per the name set in Payment Gateway Provider step
Merchant Credential	Payment (for test) / Payment_Live (for production)
Status	Set to Active to enable
Identity Type	Anonymous

d. Click Save

4. Add Trusted Sites

The endpoint URLs used by the Cybersource App need to be added to Experience Builder. Follow these steps to add the URLs listed below:

a. Click on App Launcher > Commerce

b. Select Store Record

c. Select Experience Builder > Setting > Security & Privacy > Add Trusted Site

d. Add the following URLs:

URL	Description
https://apitest.cybersource.com	Cybersource Test Endpoint
https://api.cybersource.com	Cybersource Production Endpoint
https://testflex.cybersource.com	Flex key generation for Test
https://flex.cybersource.com	Flex key generation for Production
https://centinelapistag.cardinalcommerce.com	3-D Secure Device Data Collection URL for Test
https://centinelapi.cardinalcommerce.com	3-D Secure Device Data Collection URL for Production

5. Configure Permission Set Assignment

a. For Admin User:

Permissions need to be added to the Admin User for our app to function

- i. Click Setup > Users
- ii. Select Admin user and click Edit Assignments on Permission Set Assignment
- iii. Add All Classes, Payment Configuration Access, and Order Management Operations Manager

b. For Customers:

Check that Person Account and Buyer users have the All Classes permission enabled.

6. Set Payment Configuration

a. Go to App Launcher > Set Payment Configuration and click New

b. Enter the following details:

- **Store Name:** Select the name of the store the configuration is going to be applied to
- **Endpoint:** Choose TEST or PRODUCTION (live)
- **Merchant ID:** The transacting Merchant ID (MID) assigned to you by Visa Acceptance Solutions.
- **Key ID:** The Key from your REST API Shared Secret Key
- **Shared Key:** The Shared Secret from your REST API Shared Secret Key
- **Developer ID:** Enter NONE
- **Allowed Card Networks:** Select the card brands you want to accept.
- **Enable 3DS Payment:** Check this checkbox to turn on Payer Authentication/3-D Secure
- **Enable Save Card:** Check this checkbox to allow your customers to save their cards for future transactions. Additional steps are required to support this in your B2B/ D2C store. Please see Tokenization for details
- **Enable CVV:** Check this checkbox to request customers enter their card's security code when paying with a saved card
- **ReturnUrl Page:** Enter the name of the page created in Experience Builder. See Payer Authentication for details on how to do this. This is required if you are enabling 3-D Secure.

The Cybersource Payments App is now configured and ready for use.



Note: If you are using Tokenization or Payer Authentication, you need to allocate session cache. Please see the Platform Cache section for details.

Payer Authentication

Additional configuration steps required when enabling 3-D Secure in Payment Configuration.

If you have enabled 3-D Secure in Payment Configuration, the following additional steps need to be followed.

1. Create returnUrl_Page

A returnUrl_Page needs to be created to allow for the 3-D Secure interaction to function.

- a. Go to App Launcher > Commerce and select the appropriate Store Record
- b. Click Experience Builder
- c. Select Home and then click on New Page
- d. Select Standard Page and then click on New Blank Page
- e. Select Flexible Layout and click Next
- f. Name the page then click Create
- g. Once the page is created, click Component Selection and drag payerAuth Component to the page
- h. Click Publish

2. Create New Theme Layout (B2B Aura only)

This step is required for users of B2B Aura only

- a. Go to App Launcher > Commerce and select the appropriate Store Record
- b. Click Experience Builder
- c. Select Home then go to settings > theme > configure > new theme layout. Set the name as B2B3DSNavigationLayout and select the NavigationLayoutfor 3DSB2B theme layout component
- d. Click Save
- e. Navigate to response page and click on the gear icon to open Page Properties
- f. Check Override the default theme layout for this page then select B2B3DSNavigationLayout as the Theme Layout
- g. Click Publish

Payer Authentication (3-D Secure) is now configured and ready for use with your Salesforce store.

Tokenization

Additional configuration steps required when enabling Save Card (tokenization) in Payment Configuration.

If you have enabled Save Card (tokenization) in Payment Configuration the following additional steps need to be followed.

1. Create Custom Labels

- a. Click Setup > Custom Labels
- b. Create the following custom labels:
 - Delete_Customer_Payment_Instrument_URL with the value `https://apitest.cybersource.com/tms/v2/customers/`
 - Delete_Customer_Payment_Instrument_URL_Prod with the value `https://api.cybersource.com/tms/v2/customers/`
 - Payment_Instruments with the value `/payment-instruments/`

2. Create Lightning Record

Create a Lightning Record that allows saved cards to be updated or deleted.

- a. Open any Account Record
- b. Click on Setup Menu then Edit Page
- c. Select Related Tab and then Add Tab
- d. Select Custom and set the Custom Label as Card Details
- e. Click Done
- f. From the Components panel, search for pTS_savedPaymentMethodsB2B and savedPaymentMethods and drag them to the Card Details tab
- g. Click Save
- h. Click on Activation. If you have no specific requirements, choose Assign as Org Default

Tokenization is now configured, allowing customers to save their payment methods for future transactions.

Message Level Encryption

Configuration and setup for Message Level Encryption using certificates for enhanced security.

Overview

Message Level Encryption uses certificates that ensures 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.



Note: Message Level Encryption is currently only supported for B2B Aura

Prerequisites

Using Message Level Encryption requires a .p12 certificate to be created. See [here](#) for details

Upload Certificate

1. Convert the p12 certificate to .pem format using this command:

```
openssl pkcs12 -in <key filename>.p12 -cacerts -nokeys -out cert.pem
```

2. Upload the .pem file in Static Resources:

- a. Click Setup > Static Resources
- b. Click New, enter a unique name and upload the .pem file
- c. Click Save

Enable Message Level Encryption

1. Go to App Launcher > Set Payment Configuration and choose the configuration that MLE needs to be enabled for
2. Enable Message Level Encryption: Check checkbox to enable
3. RESTCertificate (keyFileName): Add the name of the static resource given when uploading the certificate



Note: If you enable Message Level Encryption, you need to allocate session cache. Please see the Platform Cache section for details.

Platform Cache

Configure session cache allocation required for Tokenization and Payer Authentication features.

Session cache allocation is required when using Tokenization or Payer Authentication features.

Configure Platform Cache

- a. Click Setup > Platform Cache
- b. Click New and label as AccessToken
- c. Set Session Cache Allocation > Provider Free to 3

Platform Cache is now configured to support Tokenization and Payer Authentication features.

Checkout Page

Configure checkout flow for both Aura and LWR templates to use the Cybersource payment components.

The checkout flow needs to be configured differently depending on whether you are using Aura or LWR templates.

1. Configure Aura Templates

For a B2B Store using the Aura templates, the checkout flow needs to be amended to use our custom payment component using the following steps:

- a. Go to App Launcher > Commerce
- b. Select the required Store Record then click Experience Builder
- c. Select Checkout and then drag the pageReloader component to the content header
- d. Drag checkout flow template updated flow to content
- e. Click Publish

2. Configure LWR Templates

For store using LWR templates, the checkout flow needs to be amended to use our custom payment component using the following steps:

- a. Go to App Launcher > Commerce
- b. Select the required Store Record then click Experience Builder
- c. Select Checkout and then drag the Layout:Accordion component to the header section
- d. Drag the custom component D2C Payment Component to the payment section
- e. Drag Place Order standard button below the D2C Payment Component section
- f. Click Publish

The checkout page is now configured to use the Cybersource payment components for processing payments.

Order Management

Configure Order Management Lite to support Capture, Refund, and Authorization Reversal operations.

Capture and Refund are natively supported within Order Management Lite. To add support for Authorization Reversal, the component needs to be added to the Order Summary Lightning Record page.

Add Authorization Reversal Component

- a. Open any Order Summary record
- b. Click on Setup Menu and select Edit Page
- c. In the Components section, search for pTS_authReversal and drag it into the page
- d. Click Save
- e. Click on Activation. If you have no specific requirements, choose Assign as Org Default

Order Management is now configured with support for Capture, Refund, and Authorization Reversal operations.

Support & Troubleshooting

Information required when requesting support for the Cybersource Payments App.

Getting Support

If you require support with this App, please sign into the Support Center to raise a case, providing the following details:

- Summary of the issue
- Steps needed to reproduce the issue
- App version – you can check this by going to Org > Setup > Package Manager > Installed Packages
- Platform Merchant ID
- Configuration screenshots including Payment Gateway Configuration
- Debug and Payment Gateway Logs. These can be downloaded from Setup > Debug Logs
- Any other data or screenshots related to the issue

Upgrade

Instructions for upgrading to a later version of the Cybersource Payments App.

To upgrade to a later version of our app, please follow the steps provided by Salesforce.

Follow Salesforce upgrade procedures

Refer to the official Salesforce documentation for upgrading installed packages and apps in your organization.

Your Cybersource Payments App will be upgraded to the latest version with new features and improvements.