Cybersource REST Cartridge for Salesforce B2C Commerce

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

Restricted Rights Legends

Trademarks

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: **09/2024**

Contents

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:** Payment Processing, Fraud Detection, Address Validation, Tax Computation
- **Version:** 24.4.0
- **Supports Storefront Reference Architecture (SFRA) v7.0.**
- **JavaScript Controllers Friendly: YES**

Contact: globalpartnersolutionscs@visa.com

2. Cybersource SFRA Cartridge Architecture

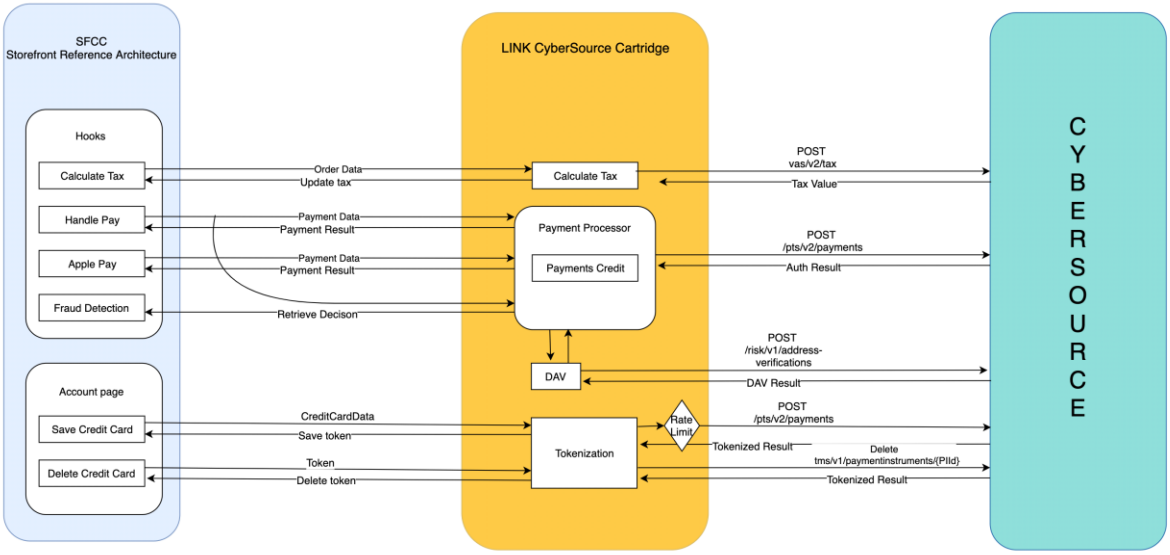

Fig 1: SFRA Cartridge Architecture

3. Install the Cartridge and Setup Workspace

3.1. Install the Cartridge

Cybersource's REST Cartridge for Salesforce B2C Commerce can be downloaded from the Salesforce AppExchange
https://appexchange.salesforce.com/appxListingDetail?listingId=a0N4V00000GbAG9UAN&tab=r.

3.2. Setup workspace

- Create a folder "Cybersource" in your workspace and place the cartridge (**int_cybs_sfra** and **int_cybs_sfra_base**) downloaded from Marketplace.
- If the project's base path is different from the one available in Cybersource's package.json , you will need to open the file '/package.json' and modify the paths.base value to point to your 'app_storefront_base' cartridge. This path is used by the JS and SCSS build scripts.
- If using VSCode install the extension Prophet Debugger link or any other SFCC extension and include below in dw.json ().

```
{
    "hostname": "your-sandbox-hostname.demandware.net",
    "username": "yourlogin",
    "password": "yourpwd",
    "version": "version_to_upload_to",
    "cartridge": [
        "int_cybs_sfra",
        "int_cybs_sfra_base",
        "app_storefront_base",
        "modules"
    ]
}
```

NOTE: If you are using different IDE, refer respective developer guide to setup the workspace.

3.3. Build and Upload the code

Prerequisite: install node under "Cybersource" folder.

Install sgmf-scripts and copy-webpack-plugin

Install sgmf-scripts and copy-webpack-plugin with following command

Command: npm install sgmf-scripts && npm install copy-webpack-plugin

Compile the Code

Compile JS and SCSS with following command

Command: npm run compile:js && npm run compile:scss

Upload the code

Upload the code to Salesforce Commerce Cloud instance

Command: npm run uploadCartridge

4. Configure the Cartridge

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.

4.1. Setup Cartridge Path

To set up the cartridge path:

- In the Business Manager, go to **Administration > Sites > Manage Sites > [yourSite] > Settings.**
- For the Cartridges, enter **int_cybs_sfra:int_cybs_sfra_base:app_storefront_base** and select **Apply.**

4.2. Upload metadata

The Cybersource Cartridge contains metadata that needs to be imported.

1. Go to **Cybersource/metadata/payments_metadata/sites/** folder.
2. Rename **yourSiteID** folder name with your site ID in Business Manager (this can be found by looking up **Administration->Sites->Manage Sites**) .
3. Zip **payments_metadata** folder.
4. Go to **Administration->Site Development->Site Import & Export** and upload **payments_metadata.zip** file.
5. Import the uploaded zip file.

On successful import, it creates following metadata:
- Site Preferences (Cybersource_Core, Cybersource_ _DeliveryAddressVerification, Cybersource_DeviceFingerprint, Cybersource_FlexMicroform, Cybersource_PayerAuthentication, Cybersource_TaxConfiguration, Cybersource_Tokenization, Cybersource_DecisionManager)
- Service (PaymentHttpService)
- Payment Processor (Payments_Credit)
- Payment Method
- Job (Payment: Decision Manager Order Update)

4.3. Cybersource Core (Required)

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/Core.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource Core** and set values for the following parameters:

Field	Description
Enable Cybersource Cartridge	Enable or disable Cybersource Cartridge. If disabled none of the Cybersource services are invoked
Cybersource MerchantID	Cybersource Merchant ID
Cybersource REST KeyId	Cybersource REST Key ID
Cybersource REST Secret Key	Cybersource REST Secret Key

Developer ID	Unique identifier generated by Cybersource for System Integrator
CardTransactionType	Select Sale/Auth transaction type
CommerceIndicator	Select MOTO/Internet

Table 1: Cybersource Core preferences

4.4. Services (Required)

Step 1: Upload Cybersource metadata in Business Manager. If not follow "**4.2: Upload metadata**" or import **"metadata/payment_metadata/meta/Payment-Services.xml"** in Business Manager (**Administration > Operations > Import & Export**).

Step 2: Go to **Administration > Operations > Services** and click on the **Payment Credentials** of the service.

Step 3: Make sure the URL are appropriate.

Environment	URL
Test	https://apitest.cybersource.com
Production	https://api.cybersource.com

Table 2: Service endpoints

4.5. Payment Processor (Required)

Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/sites/yourSiteID/payment-processors.xml" in Business Manager (Merchant Tools > Ordering > Import & Export).

5. Configure the Payment method

5.1. Credit Card

In the Business Manager, go to **Merchant Tools > Ordering > Payment Methods** and select **CREDIT_CARD**. And in **CREDIT_CARD details**, double check if **Payment Processor** = **"PAYMENTS_CREDIT".**

The Cybersource Cartridge supports the following payment card capture methods:

a. Microform 0.11
b. Direct API

Please note that selecting Direct API will increase your PCI DSS scope

5.1.1 To Setup Microform 0.11

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/FlexMicroform.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_FlexMicroform** and set values for the parameter:

Field	Description	Value to Set
Enable Secure Acceptance - Flex Microform	Enable or Disable Cybersource Flex Microform Service	Yes

Table 3: Cybersource Microform Preference

5.1.2 To Setup Direct Cybersource Payment API

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/FlexMicroform.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_FlexMicroform** and set the value for following parameter:

Field	Description	Value to Set
Enable Secure Acceptance – Flex Microform	Enable or Disable Cybersource Flex Microform Service	No

Table 4: Cybersource Microform Preference

5.1.3. Payer Authentication (3D Secure)

Prerequisite

If you wish to process card payments with Payer Authentication, please ensure your Cybersource account has been enabled for it. Please contact your Cybersource representative if you are unsure.

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/PayerAuthentication.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_PayerAuthentication** and set values for the following parameters:

Field	Description
Enable Payer Authentication	Enable or Disable Payer Authentication service

Table 5: Cybersource PayerAuthentication Preferences

Enforce Strong Consumer Authentication

When Payer Authentication is enabled, if a transaction gets declined with the reason as Strong Customer Authentication required, then another request will be sent from cartridge automatically for the same order and the customer will be 3DS challenged.

In case merchants would like the cardholder to be 3DS Challenged when saving a card, IsSCAEnabled setting can be updated to enable it for credit cards.

Note: The scaEnabled setting is applicable only if Payer Authentication is enabled.

Site Preferences:

Step 1: Upload Cybersource metadata to Business Manager. If not follow "4.2: Upload metadata" or import "metadata/sfra_meta/meta/PayerAuthentication.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_PayerAuthentication** and set values for the following parameters:

Field	Description
IsSCAEnabled	Enable Strong Customer Authentication

Table 6: Cybersource SCA Preference

Set the value for IsSCAEnabled to yes to use Strong Customer Authentication feature.

Decision Manager with Payer Authentication

Decision Manager plus Payer Authentication allows pre-authentication rules to be configured before authentication takes place, providing EMV®*3* 3DS authentication and risk review from authentication to authorization.

Site Preferences:

Step 1: Upload Cybersource metadata to Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/PayerAuthentication.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_PayerAuthentication** and set values for the following parameters:

Field	Description
Enable Payer Authentication	Enable or Disable Payer Authentication service

Table 7.1: Cybersource PayerAuthentication Preferences

Step 2.1: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_DecisionManager** and set values for the following parameters:

Field	Description
Enable Decision Manager Services	Enable or Disable Decision Manager for Cybersource Cartridge

Table 7.2: Cybersource Decision Manager Preference

5.2. Apple Pay

5.2.1. Create a merchant identifier in Apple portal

A merchant identifier uniquely identifies you to Apple Pay as a merchant who is able to accept payments. You can use the same merchant identifier for multiple native and web apps. It never expires.

- Go to Apple portal : https://developer.apple.com
- In Certificates, Identifiers & Profiles, select Identifiers from the sidebar, then click the Add button (+) in the upper-left corner.
- Select Merchant IDs, then click Continue.
- Enter the merchant description and identifier name, then click Continue.
- Review the settings, then click Register.

5.2.2. Enrolling in Apple Pay in Cybersource

To enroll in Apple Pay:

- Log in to the Business Center:
  - Test: https://ebctest.cybersource.com/ebc2/
  - Live: https://ebc2.cybersource.com/ebc2/
- On the left navigation pane, click the **Payment Configuration** icon.
- Click **Digital Payment Solutions**. The Digital Payments page appears.
- Click **Configure**. The Apple Pay Registration panel opens.
- Enter your Apple Merchant ID. (Created in Step 1.4)
- Click **Generate New CSR**.
- To download your CSR, click the **Download** icon next to the key.
- Follow your browser's instructions to save and open the file.

5.2.3. Complete the enrollment process by submitting your CSR to Apple

Create a payment processing certificate: A payment processing certificate is associated with your merchant identifier and used to encrypt payment information. The payment processing certificate expires every 25 months. If the certificate is revoked, you can recreate it.

- In Certificates, Identifiers & Profiles, select Identifiers from the sidebar.
- Under Identifiers, select Merchant IDs using the filter in the top-right.
- On the right, select your merchant identifier. Note: If a banner appears at the top of the page saying that you need to accept an agreement, click the Review Agreement button and follow the instructions before continuing.
- Under Apple Pay Payment Processing Certificate, click Create Certificate.
- Click Choose File.
- In the dialog that appears, select the CSR file downloaded from Step 2.7, then click Choose.
- Click Continue.

5.2.4. Configure Apple Pay in SFCC Business Manager

Business Manager Configuration

- Go to: **"Merchant Tools > Site Preferences > Apple pay.**
- Check "Apple Pay Enabled?"
- Fill in the "Onboarding" form:
  - Ensure "Apple Merchant ID" and "Apple Merchant Name" match settings in your Apple account.
  - Ensure all other fields match the your supported Cybersource settings.
- Fill in the "Storefront Injection" form:
  - Selects where Apple Pay buttons should be displayed on your site.
- Fill in "Payment Integration" form:
  - Leave all form fields blank.
  - Ensure "Use Basic Authorization" is checked
- Click "Submit".

5.2.5. Domain Registration in SFCC Business Manager

- Go to: **"Merchant Tools > Site Preferences > Apple Pay.**
- Under **Domain Registration** section
  - Click on **Register Apple Sandbox** under Apple Sandbox section for registering SFCC to Apple Sandbox account.
  - Click on **Register Apple Production** under Apple Production section for registering SFCC to Apple Production account.

5.2.6. Payment Processor

In the Business Manager, go to **Merchant Tools > Ordering > Payment Methods** and select **DW_APPLE_PAY**. And in **DW_APPLE_PAY details**, double check if **Payment Processor** = **"PAYMENTS_CREDIT".**

Site Preferences:

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import **"metadata/sfra_meta/meta/ApplePay.xml"** in Business Manager (**Administration > Site Development > Import & Export**).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Apple Pay** and set values for the following parameters:

Field	Description
ApplePayTransactionType	Select Sale/Auth transaction type

Table 7: Cybersource Apple Pay Preference

5.3. Google Pay

5.3.1. Create custom preference for Google Pay

- Upload Cybersource metadata in Business Manager. If not follow "**4.2: Upload metadata**" or import **"metadata/payment_metadata/meta/GooglePay.xml"** in Business Manager (**Administration > Site Development > Import & Export**).

- Go to **Merchant Tools > Site Preferences > Custom Preferences > Google Pay** and set values for the following parameters:

Field	Description
Enable Google Pay	Enable/Disable Google Pay on checkout page
Enable Google Pay on Mini Cart	Enable/Disable Google Pay on mini cart
Enable Google Pay on Cart	Enable/Disable Google Pay on cart page
Google Pay Merchant Id	Merchant Id required for Live Environments
Google Pay Environment	Environment details of Google Pay. Possible values are Test or Production
Google Pay Transaction Type	Select Sale/Auth transaction type

Table 8: Cybersource Google Pay Preferences

5.3.2. Payment Processor

In the Business Manager, go to **Merchant Tools > Ordering > Payment Methods** and select **DW_GOOGLE_PAY**. And in **DW_GOOGLE_PAY details**, double check if **Payment Processor** = **"PAYMENTS_CREDIT".**

5.3.3. Request Production Access

If you want to use Google Pay in **LIVE Environment**, then navigate to this link https://pay.google.com/business/console/ to get Google Pay merchant Id.

5.4. Click to Pay

5.4.1. Create custom preference for Click to Pay

- Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import **"metadata/payment_metadata/meta/VisaSRC.xml"** in Business Manager (**Administration > Site Development > Import & Export**).

- Go to **Merchant Tools** > **Site Preferences > Custom Preferences > Click to pay** and set values for the following parameters:

Field	Description
Enable Click to Pay	Enable/Disable Enable Click to Pay on checkout page
Click to Pay Key	Click to Pay Key Id obtained through EBC Digital payments
True for production	Set to Yes for Production
Click to Pay Transaction Type	Select Sale/Auth transaction type

Table 9: Cybersource Click to Pay Preferences

5.4.2. Payment Processor

In the Business Manager, go to **Merchant Tools > Ordering > Payment Methods** and select **CLICK TO PAY**. And in **CLICK_TO_PAY details**, double check if **Payment Processor** = **"PAYMENTS_VISA_SRC".**

Note: Currently Click to Pay is only available in checkout view.

6. Configure Features

6.1. Token Management Service

Refer to this link to learn about Cybersource's Token Management service

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/Tokenization.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools** > **Site Preferences** **> Custom Preferences > Cybersource_Tokenization** and set values for the following parameters:

Field Name	Description
Enable Tokenization Services	Enable or Disable the Tokenization Service saving Credit/Debit Card on "My Account" page
Enable limiting Saved Card	Enable or Disable limiting Saved Card on My Account page
Saved Card Allowed	Number of Cards that can be added in a defined interval on My Account page
Reset Interval (in Hours)	Number of hours that saved card attempts are counted

Table 10: Cybersource Tokenization Preferences

NOTE: If you want to utilize **"save card to account"** feature through "Payment flow/Checkout flow", make sure to set **"Enable tokenization Services"** to **"Yes".**

6.2. Network Tokens

A Network Token is a card scheme generated token, that represents customer card information for secure transactions that references a customer's actual PAN.

Your Cybersource Merchant ID needs to be enabled for Network Token's before you can use this service. Please contact your Cybersource representative to request enablement.

The Cybersource cartridge will subscribe to the Token Life Cycle web hook and make the necessary updates to the saved card details.

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payments_metadata/meta/Tokenization.xml". and "metadata/payments_metadata/meta/custom-objecttype-definitions.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_Tokenization** and set values for the following parameters:

Field Name	**Description**
Enable Tokenization Services	Enable or Disable the Tokenization Service saving Credit/Debit Card

	on “My Account” page
Network Token Updates	Subscribe to Network Token life cycle updates

Table 11: Cybersource Network Tokens Preference

Step 3: Go to **Merchant Tools > Custom objects > Custom Object Editor** and check if the custom object type "Network Tokens Webhook" exists without any object.

A custom object of this type would be created only if the Network Tokens webhook is subscribed.

NOTE: To utilize Network Tokens feature

- Make sure “Enable Tokenization Services” and “Network Token Updates” are set to yes.
- The Webhook URL needs to be added in the following path “Payment Configuration > Webhook Settings > Configure in the Business Centre and make sure its enabled.
- The Webhook URL needs to be in the following format: {Hostname}/WebhookNotification-tokenUpdate.

For E.g., https://zzkm.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/default/WebhookNotification-tokenUpdate

6.3. Delivery Address Verification

Step 1: Upload Cybersource metadata in Business Manager. If not follow “4.2: Upload metadata” or import “metadata/payment_metadata/meta/DeliveryAddressVerification.xml” in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_DeliveryAddressVerification** and set values for the parameter:

Field	Description
Enable Delivery Address Verification Services	Enable or Disable Delivery Address Verification for Cybersource Cartridge

Table 12: Cybersource Delivery Address Verification Preference

6.4. Tax Calculation

Step 1: Upload Cybersource metadata in Business Manager. If not follow “4.2: Upload metadata” or import “metadata/payment_metadata/meta/TaxConfiguration.xml” in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_TaxConfiguration** and set values for the following parameters:

Field	Description
Enable Tax calculation Services	Enable or disable Cybersource tax service for Cybersource Cartridge
List of nexus states	When your company has nexus in the U.S. or Canada, you might be required to collect sales tax or seller’s use tax in those countries
List of nexus states to	List of nexus states to exclude

exclude	
Merchant's VAT Registration Number	A VAT seller registration number is required in order to calculate international taxes and might be required for some Canadian transactions. International/VAT calculation is supported in specific countries
Default Product Tax Code	Default tax code used when tax code is not set on a product
Purchase Order Acceptance City	Purchase order acceptance city
Purchase Order Acceptance State Code	Purchase Order Acceptance State Code. Use the State, Province, and Territory Codes for the United States and Canada
Purchase Order Acceptance zip code	Purchase Order Acceptance zip code
Purchase Order Acceptance Country Code	Purchase Order Acceptance Country Code. Use the two-character ISO Standard Country Codes
Purchase Order Origin City	Purchase Order Origin City
Purchase Order Origin State Code	Purchase Order Origin State Code. Use the State, Province, and Territory Codes for the United States and Canada
Purchase Order Origin Zip Code	Purchase Order Origin Zip Code
Purchase Order Origin Country Code	Purchase Order Origin Country Code. Use the two-character ISO Standard Country Codes
Ship From City	Ship From City
Ship From State Code	Ship From State Code
Ship From Zip Code	Ship From Zip Code
Ship From Country Code	Ship From Country Code

Table 13: Cybersource Tax Configuration Preferences

6.5. Fraud Management Solutions

Refer to this link to learn about Cybersource's Decision Manager and Fraud Management Essentials. Both services use the same cartridge settings and fields, to access the service a retailer has signed up for with Cybersource.

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/DecisionManager.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_DecisionManager** and set values for the following parameter:

Field	Description

Enable Decision Manager Services	Enable or Disable Decision Manager for Cybersource Cartridge

Table 14: Cybersource Decision Manager Preference

Step 3: To enable **Decision Manager Order Update Job**: Decision Manager Order Update Job uses a REST API to retrieve order decisions from Cybersource and update the order confirmation status in SFCC.

To Integrate this job into your site, follow the below steps:
Step 3.1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/jobs.xml" in Business Manager (Administration > Operations > Import & Export).

Step 3.2: Open Business Manager. Go to **Administration > Operations > Jobs** and select **Payment: Decision Manager Order Update**. Make sure following values are filled in:

Field	Description
ID	Identifier
Description	Description
ExecuteScriptModule.Module	int_cybs_sfra_base/cartridge/scripts/jobs/DMOrderStatusUpdate.js
ExecuteScriptModule.FunctionName	orderStatusUpdate
ExecuteScriptModule.Transactional	Indicates if the script module's function requires transaction handling.
ExecuteScriptModule.TimeoutInSeconds	The timeout in seconds for the script module's function

Table 15: Cybersource DM Order Update

Step 3.3: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_DecisionManager** and set values for the following parameter:

Field	Description
Conversion Detail Report Lookback time	Number of hours the job will look back for new decisions. CS does not support lookbacks over 24 hours. Do not set above 24.

Table 16: Cybersource Decision Manager Preference

6.6. Device FingerPrint

Device FingerPrint is a powerful feature of Decision Manager and Fraud Management Essentials It is always recommended to send a Device Fingerprint when using a Cybersource fraud management service.

Step 1: Upload Cybersource metadata in Business Manager. If not follow "4.2: Upload metadata" or import "metadata/payment_metadata/meta/DeviceFingerprint.xml" in Business Manager (Administration > Site Development > Import & Export).

Step 2: Go to **Merchant Tools > Site Preferences > Custom Preferences > Cybersource_DeviceFingerprint** and set values for the following parameters:

Field	Description
Enable DeviceFingerprint	Enable or Disable the Device Fingerprint Service.

Service	
Organization Id	Organization ID for the device fingerprint check
Thread Matrix URL	Thread Matrix URL pointing to JS that generates and retrieves the fingerprint.
TTL (Time To Live)	Time, in milliseconds between generating a new fingerprint for any given customer session

Table 17: Cybersource DeviceFingerprint Preferences

6.7. Capture Service

A single function is available to make capture requests. Please note that these functions are not available to use in the Salesforce B2C Commerce UI without customisation

```
httpCapturePayment(requestID, merchantRefCode, purchaseTotal, currency)
```

This function can be found in the script **'scripts/http/capture.js'**. A working example of how to use this function can be found in the **ServiceFrameworkTest-TestCaptureService** controller. You will first get an instance of the capture.js object, and make the call as follows:

```
var captureObj = require("~/cartridge/scripts/http/capture.js");
var serviceResponse = captureObj.httpCapturePayment(requestID, merchantRefCode,
paymentTotal, currency);
```

The resulting serviceResponse object will contain the full response object generated by the request. The contents of this object will determine your logic in handling errors and successes. For detailed explanations of all possible fields and values, refer this link .

Capture Request Parameters

Parameter Name	Description
requestID	Transaction ID obtained from the initial Authorization
merchantRefCode	SFCC Order Number
purchaseTotal	Order Total
currency	Currency code (ex. 'USD')

Table 18: Capture Request Parameters

6.8. Auth Reversal Service

A single function is available to make auth reversal requests. Please note that these functions are not available to use in the Salesforce B2C Commerce UI without customisation .

```
httpAuthReversal(requestID, merchantRefCode, amount, currency)
```

This function can be found in the script **'scripts/http/authReversal.js'**. A working example of how to use this function can be found in the **ServiceFrameworkTest- TestAuthReversal** controller. You will first get an instance of the AuthReversal.js object, and make the call as follows:

```
var reversalObj = require("~/cartridge/scripts/http/authReversal.js");
var serviceResponse = reversalObj.httpAuthReversal(requestID, merchantRefCode,
paymentTotal, currency);
```

The resulting serviceResponse object will contain the full response object generated by the request. The contents of this object will determine your logic in handling errors and successes. For detailed explanations of all possible fields and values, refer this link

Authorization Reversal Request Parameter

Parameter Name	Description
requestID	Transaction ID obtained from the initial Authorization
merchantRefCode	SFCC Order Number
amount	Order Total
currency	Currency code (ex. 'USD')

Table 19: Authorization Reversal Request Parameter

6.9. Advanced Customization

The Cybersource SFRA cartridge has built-in custom hooks that can be utilized to customize request data being sent to each Service. This can be utilized to send additional custom data that the core cartridge cannot account for. For example, if you want to include Merchant Defined Data in your Credit Card Authorization Requests, you can use these hooks to achieve this.

The hooks are called in the **'scripts/http/capture.js'** and **'scripts/http/AuthReversal.js'** scripts. After a request for a particular service is built, but before it is sent to CS, a check for any code registering to the hook 'app.payment.modifyrequest' is done. If present, the hook will be called for that specific request. The request object is passed into the hook and the return value of the hook is sent to CS as the final request object. Through this process, you can inject your own data into the request object from custom code you write in a separate cartridge.

Implementation:
To customize request objects, register the hook **'app.payment.modifyrequest'** in your cartridges **'hooks.json'** file. An example would look like this, replacing the script path with your own script :

```
{
    "name": "app.payment.modifyrequest",
    "script": "./cartridge/scripts/hooks/modifyRequestExample"
}
```

You can copy the **'scripts/hooks/modifyRequestExample'** script from this cartridge into your own to use as a template for extending and modifying service request objects. Note, every hook must return a valid request object for the given service. It is recommended that you reference the CybserSource documentation for details on the exact nature of any fields you wish to customize or add. The following hooks are available for you to define in this file:

Modify Request hooks

Hook Name	Service Request to modify
AuthReversal	Credit Card Authorization Reversal
Capture	Credit Card Capture

Table 20: Modify Request hooks

7. Test and Go Live

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

Test your integration

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 completely separate from the live production environment, and it requires separate credentials. If you use your production credentials in the sandbox or visa versa, you get a 401 HTTP error.

Sign up for a sandbox account if you have not yet.

Use our test card numbers to make test payments: > The following test credit card numbers work only in the sandbox. If no expiration date is provided, use any expiration date after today's date. If the card verification code is required and is not provided, use any 3-digit combination for Visa, Mastercard, Discover, Diners Club and JCB; use a 4-digit combination for American Express.

Test Card Brand	Number	CVV	Expires
Visa	4111 1111 1111 1111		
Visa	4622 9431 2701 3705	838	12/22
Visa	4622 9431 2701 3713	043	12/22
Visa	4622 9431 2701 3721	258	12/22
Visa	4622 9431 2701 3739	942	12/22
Visa	4622 9431 2701 3747	370	12/22
MasterCard	2222 4200 0000 1113		
	2222 6300 0000 1125		
	5555 5555 5555 4444		
American Express	3782 8224 6310 005		
Discover	6011 1111 1111 1117		
JCB	3566 1111 1111 1113		
Maestro (International)	5033 9619 8909 17		
	5868 2416 0825 5333 38		
Maestro (UK Domestic)	6759 4111 0000 0008		
	6759 5600 4500 5727 054		

	5641 8211 1116 6669		
UATP	1354 1234 5678 911		

Table 20: Test Card details

Test card numbers for Network Tokens:

Test Card Brand	Number	CVV	Expires
Visa	4895 3799 8000 0580		
Visa	4895 3799 8000 0572		
Visa	4895 3799 8000 0564		
Visa	4895 3799 8000 0325		
MasterCard	5120 3422 3315 0747		
MasterCard	5120 3432 8749 9758		
MasterCard	5120 3501 0006 4594		
MasterCard	2222 6904 2006 4590		

Table 21: Test Card details for NT

Register SFCC sandbox to Apple Sandbox Account.

- Go to: **"Merchant Tools > Site Preferences > Apple pay.**
- Under **Domain Registration** section
  - Click on **Register Apple Sandbox** under Apple Sandbox section for registering SFCC to Apple Sandbox account.

To manage your evaluation account, log in to the Test Business Center and do the following: - View test transactions. - Access administrator users and access privileges. - Create roles with predefined access permissions. - View reports.

Important: Cybersource recommends that you submit all banking information and required integration services in advance of going live. Doing so will speed up your merchant account configuration.

Configure your live account

Once you have the credentials for the live environment:

- Configure cartridge using your live account settings.
- Test your integration

8. Upgrade Steps

Upgrade from version 24.3.0 to 24.4.0

Please follow the below steps to upgrade your cartridge version from 24.3.0 to 24.4.0.

- Please download and install Cybersource REST Cartridge for B2C Commerce from Salesforce Commerce Cloud's marketplace https://appexchange.salesforce.com/listingDetail?listingId=a0N4V00000GbAG9UAN&tab=e.
- Run **`npm i jquery@3.7.0`** and compile our cartridge using **`npm run compile:js`** and **`npm run compile:scss`**
- Upload metadata

-> The Cybersource Cartridge contains metadata that needs to be imported.
-> Go to **Cybersource/metadata/payments_metadata/sites/** folder.
-> Zip **payments_metadata** folder.
-> Go to **Administration->Site Development->Site Import & Export** and upload. **payments_metadata.zip** file.
-> Import the uploaded zip file.

9. Release Notes

Version 24.4.0 (September2024)

- Added DMPA support.
- Upgraded to jQuery v3.7.0.

Version 24.3.0 (August 2024)

- Upgraded the cartridge to support SFRA v7.0.
- Added Commerce Indicator MOTO.

Version 24.2.1 (May 2024)

- Checkmarx issues fixed.
- Device fingerprint bug fixed.

Version 24.2.0 (April 2024)

- Implemented Direct API integration for Payer Authentication with Payer Auth Setup and Device Data Collection.
- Enhanced SCA feature.
- Implemented Network Tokens feature.

Version 24.1.0 (February 2024)

- Upgraded the cartridge to support SFRA v6.3.
- Updated cartridge to make it compatible with Salesforce B2C Commerce Release 22.7.
- Added Strong Customer Authentication for Credit Card.
- Renamed Visa SRC to Click to Pay.
- Implemented Sale functionality for Credit Card, Google Pay, Click to Pay and Apple Pay.
- Updated flex script referring to from v0.11.0 to v0.11.
- Updated API header in Http Signature Authentication.

Version 21.1.0 (June 2021)

<u>New Features</u>

- Improved Payer authentication screen (modal).

<u>Bug Fixes</u>

- Added descriptive error messages on certain fail cases and invalid inputs.
- Reloading on final confirmation page does not result on failed authorization.

Version 20.2.0 (Feb 2021)

<u>New Features</u>

- Support Google Pay payment method.
- Support Visa SRC payment method.
- Improved security on “My Account” page by adding Microform approach to tokenize credit card.

<u>Bug Fixes</u>

- Improved security of keys by changing data type of password fields from “String” to “password”.
- We added more security to exposed parameters of device fingerprint.

Version 20.1.1 (Nov 2020)

<u>Bug Fixes</u>

- Improved security on accessing and modifying sensitive fulfillment-related actions on an order (e.g.,

order acceptance, canceling etc.).

Version 20.1.0 (Aug 2020)

- Support Credit Card payment using Cybersource REST Payment API and Flex Microform v0.11.
- Support Apple Pay.
- Support PayerAuth/3D Secure using Cardinal Cruise API.
- Support Tokenization on “My Account” and “Payment Page”.
- Support Delivery Address Verification service.
- Support Tax Service.
- Support Capture and Auth Reversal services.

10. Support

If you require support with this software, please contact GlobalPartnerSolutionsCS@visa.com and provide the following details:

- Summary of the issue.
- Steps to reproduce the issue.
- Cybersource B2C Commerce Plugin Version.
- Cybersource Merchant ID.
- Configuration screenshots: Please provide screenshots of Custom Preference Configurations.
- Log file and other relevant data: Download the logs from Administration -> Site Development -> Development Setup -> Log files.