

Oracle Fusion Cloud Service on OCI Payments Module PCI DSS Implementation

Follow the steps and best practices outlined in this document in order for your Oracle Fusion Cloud Service on OCI to support your PCI DSS compliance efforts. Additionally, you must consult your own PCI DSS Qualified Security Assessor (QSA) to validate PCI DSS compliance within your own organization.

Mar 2022, Version 1.9
Copyright © 2022, Oracle and/or its affiliates
Confidential – Oracle Internal

Purpose statement

This document describes the steps that must be followed in order for your Oracle Fusion Cloud Service on OCI to comply with Payment Card Industry Data Security Standards (PCI DSS) when using Oracle Fusion Payments module. The information in this document is based on PCI Security Standards Council Data Security Standards program version 3.2.1. Oracle instructs and advises its customers to implement Oracle Fusion Cloud Service on OCI in a manner that adheres to the PCI Data Security Standard (v3.2.1).

Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

For credit card processing, Oracle Fusion Payments module supports CyberSource ‘Secure Acceptance Hosted Checkout’ and ‘Tokenization’ services out of the box. The credit card processing common architecture can also be used to integrate other supported gateways for payment processing and credit card tokenization services.

For employee corporate card expense processing, Oracle Fusion Expenses module only accepts and processes either a tokenized or a truncated version of the corporate card number.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Purpose statement	2
Disclaimer	2
PCI DSS	5
Protecting Cardholder Data	5
Payment Gateway Integration	5
PayPal Integration	5
Types of Cardholder Data	6
How Cardholder data is protected	6
Tokenization	6
Encryption	7
System-Level Key	7
Oracle Platform Security Services (OPSS)	7
Data Encryption Subkeys	7
Key Rotation	7
Compromised Keys	8
Account and Password Management	8
Shared Accounts	9
User Auditing	10
Logging	10
Infrastructure	10
Network	10
Wireless	10
Maintenance	10
Security Alerts	10
Providing Diagnostic Information	11
Implementation Steps	11
Setup in CyberSource	11
CyberSource Merchant Account	11
Transaction Security Key	15
Shared Secret Key	16
Setup in Oracle Fusion Payments	17
Enabling Credit Card Feature	17
Tokenization Setup	20
Payment System Setup	21
Transmission Configuration Setup	24
Funds Capture Process Profile Setup	25
Internal Payee Setup	26
Payee Routing Rule Setup	27
System Security Option Setup	28

Credit Card Business Flows	29
UI Flow	29
UI Flow with CVV support	29
Flow for Handling Failed or Orphaned Transactions Using CyberSource Query	30
Spreadsheet Import Flow	31
Oracle Fusion Payments Card Tokens Import with Transactions	32
Corporate Card File Import Flow - Expenses	32
Pay via PayPal flows	33

PCI DSS

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

Important: To stay PCI DSS compliant, you must never send a corporate card file that contains corporate card numbers that aren't tokenized or truncated to Oracle Fusion Expenses module for employee expense processing.

Protecting Cardholder Data

When Oracle Fusion Cloud Service on OCI Payments module is implemented according to the information in this document, it facilitates and supports the Payment Card Industry Data Security Standard version 3.2.1 requirements. This section provides an overview of the security features in Oracle Fusion Payments that are responsible for protecting cardholder data.

Payment Gateway Integration

A fundamental component of the Payments module's PCI DSS strategy is the tokenization of all payment card Primary Account Numbers (PANs) through integration with supported gateways such as CyberSource.

To make CyberSource ready-to-use, Oracle Fusion Payments utilizes the following services for card tokenization, card verification value (CVV) tokenization, storage, and payment processing:

- Secure Acceptance Hosted Checkout
- Tokenization Service (for card and CVV*)

Note: Tokenization Service securely passes the credit card security code (CVV) through a flex-microform to CyberSource for card-on-file transactions and stores only the transient CVV token (in-memory), issued by CyberSource.

CyberSource provides payment processing services to enable customers to connect with various payment processors. The service complies with the latest security and connectivity requirements for credit transactions as stipulated by PCI.

Refer to the following link for more information on CyberSource product documentation.

- <https://www.CyberSource.com/developers/documentation/>

Just like CyberSource, other payment gateways can also be integrated with Fusion Payments. The payment gateway redirects to a hosted order page that takes in the credit card information, tokenization of PAN number, and CVV as well as the credit card processing.

Important: The common architecture of Oracle Fusion Payments module lets you integrate with the payment gateway of your choice. However, while choosing the payment gateway for credit card tokenization and payment processing, you must ensure the following:

1. The payment gateway provides a tokenization scheme where the original PAN (credit card number) cannot be computed simply by knowing only the token or a number of tokens.
2. The PAN (credit card number) and the Sensitive Authentication Data (SAD) must not be transmitted back to Oracle.
3. The credit card data entry page of the payment gateway must be encapsulated in an iframe so that the entered credit card data never comes in contact with the Oracle systems.

PayPal Integration

Oracle Fusion Payments allows users to make payments through PayPal checkout in Oracle Public Sector Compliance and Regulation (PSCR) service. PSCR is a cloud application within Fusion SCM suite which integrates with PayPal by utilizing their Express Checkout product.

Types of Cardholder Data

As per PCI DSS guidance, entities accepting payment cards are expected to protect cardholder data and to prevent its unauthorized use – whether the data is printed, stored locally, or transmitted over an internal or public network to a remote server or service provider. Oracle Fusion Cloud Service on OCI Payments partners with CyberSource to provide secure cardholder data storage and funds capture processing functionality. The following table lists the various types of PCI DSS cardholder data and their data stages within Oracle Fusion Cloud Service on OCI.

DATA TYPE	RECEIVED	STORED	PROCESSED	PRESENTED	EXTERNALLY TRANSMITTED
Credit card Primary Account Number (PAN)	N/A	N/A	N/A	N/A	N/A
Credit card verification number (or Card Verification Value or CVV)	N/A	N/A	N/A	N/A	N/A
Payment instrument magnetic track data	N/A	N/A	N/A	N/A	N/A
External system access information, such as login passwords*	X	X	X	N/A	X

* Based on using a federated approach to satisfy Account & Password Management processes

The following information describes the stages of the PCI DSS data types:

- **Received:** An entry point for data. It is accepted as a parameter of an API or functional process and only retained in volatile storage, such as computer memory.
- **Stored:** Permanent storage, such as the database or a file system.
- **Processed:** Accessed internally by Oracle Fusion Payments in a plain text (decrypted) format, but not communicated outside the processing module.
- **Presented:** Plain text of the data presented through an electronic form, rather than a truncated or masked form.
- **Externally Transmitted:** Delivery of data to an external system, typically through electronic network communication.

How Cardholder data is protected

Tokenization

Tokenization is the process of storing sensitive data, such as credit card numbers and CVV in an external, centralized, and secure data vault. A token value replaces sensitive data in the database and in external communications, such as authorizations and settlements.

Oracle Fusion Cloud Service on OCI only stores a CyberSource-generated token for the PAN in database and a transient token (in-memory) for CVV. A display-only, masked version of the truncated PAN is also stored. The truncated PAN complies with all PCI DSS requirements and stores only the last four digits of the PAN.

Oracle Fusion Payments supports token length up to 30-characters. When you implement tokenization, choose a token format that doesn't exceed this limit. If you are using CyberSource, don't use the default token format of 32-character hexadecimal. Instead, choose a token format with numeric characters with length below 30-digits. For more information, visit the CyberSource Token Management Service Using the Simple Order API guide.

- http://apps.CyberSource.com/library/documentation/dev_guides/Token_Management/SO_API/TMS_SO_API.pdf

Oracle Fusion Cloud Service on OCI Payments module never displays the CyberSource token. Instead, it displays a masked card number returned by CyberSource with only the last four digits of the PAN. After you enable tokenization, credit card masking settings are no longer modifiable, and the last 4-digit display option is fixed for all user roles. No user role is allowed to view the full PAN.

For CVV, user enters it in the CyberSource owned flex micro-form rendered on Oracle Fusion Payments Cloud. CyberSource generates a transient token for the entered CVV in the JavaScript layer. This transient token is stored in memory and used for authorization in the same session.

Encryption

Encryption is the encoding of sensitive data, such as credit card numbers, so that they cannot be read or copied. Oracle Fusion Payments protects non-PCI data with application-level encryption. Non-PCI data includes CyberSource and non-CyberSource security credentials. The architecture is comprised of the following components:

- System-level key
- Oracle Platform Security Services (OPSS) credential and key storage
- Data encryption subkeys
- Secure data segments storage

System-Level Key

When you enable application-level encryption in the Payments module of the Oracle Fusion Cloud Service on OCI, you create a system-level security key. The system-level security key is a randomly generated Advanced Encryption Standard (AES) cipher encryption key. You can rotate the system key, which secures the data encryption subkeys.

Oracle Platform Security Services (OPSS)

OPSS provides security-related services for Oracle Public Cloud Applications. The OPSS key store is the secure storage repository for the Payments system-level key. The OPSS credential store is the secure storage repository for external passwords.

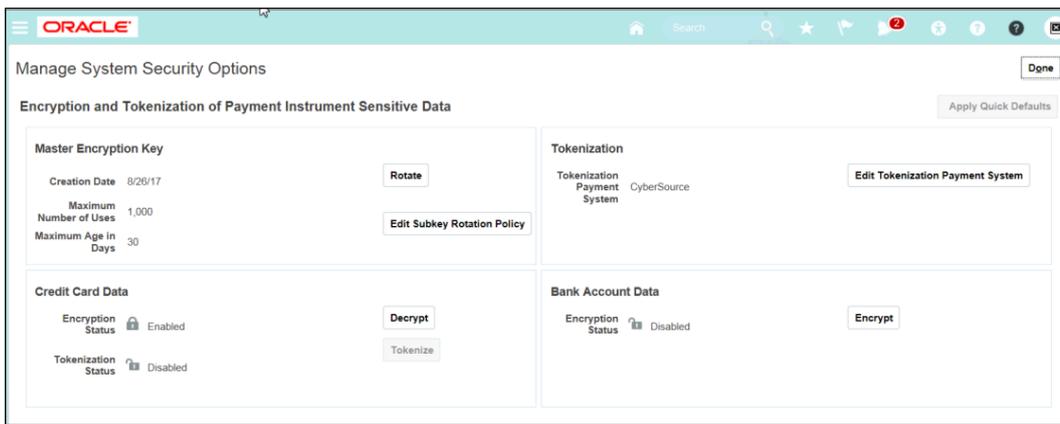
Data Encryption Subkeys

Data encryption subkeys are randomly generated symmetric cipher keys that are encrypted using the system-level key. Oracle Fusion Cloud Service on OCI Payments module does not store the subkeys in unencrypted format. Subkeys encrypt access and security credentials. The system automatically manages the creation and encryption of the subkeys.

Key Rotation

According to the PCI DSS standard, key rotation must occur once the keys have reached the end of their defined crypto period. Key rotation results in the immediate re-encryption of all data encryption subkeys by the new master encryption key. To secure your payment instrument data, perform rotation of the master encryption key regularly. Rotating the master encryption key generates a new one.

To rotate the master encryption key, click Rotate on the Manage System Security Options page.



Rotating the master encryption key

Compromised Keys

In the event of a suspected or confirmed compromised master encryption key or data encryption subkey, contact Oracle Support.

Account and Password Management

Oracle Fusion Cloud Service on OCI allows the use of federation to a customer's own authentication and authorization identity provider or to Oracle Identity Cloud Service (IDCS) in order to meet PCI DSS requirements for account and password management.

When federating to your identity provider solution, you have a responsibility to meet the PCI DSS requirements for Password Management as outlined below. Consult your own QSA for additional details and clarifications.

PCI DSS Requirement #	Requirement language and description
8.1 (8.1.1 – 8.1.8)	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.6.b	Review internal processes and customer/user documentation, and observe implemented processes to verify that <i>non-consumer</i> customer user accounts are temporarily locked-out after not more than six invalid access attempts
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
8.2 (8.2.1 – 8.2.6)	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
8.2.3	Passwords/passphrases must meet the following: <ul style="list-style-type: none"> • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.
8.2.3.b	Review internal processes and customer/user documentation to verify that <i>non-consumer</i> customer password/passphrases are required to meet at least the following strength/complexity: <ul style="list-style-type: none"> • Require a minimum length of at least seven characters • Contain both numeric and alphabetic characters
8.2.4	Change user passwords/passphrases at least once every 90 days.
8.2.4.b	Review internal processes and customer/user documentation to verify that: <ul style="list-style-type: none"> • <i>Non-consumer</i> customer user passwords/passphrases are required to change periodically • <i>Non-consumer</i> customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
8.2.5.b	Review internal processes and customer/user documentation to verify that new <i>non-consumer</i> customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
8.3 (8.3.1 – 8.3.2)	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

When federating back to your own identity provider solution, you can find the instructions at the following documentation link:

- Configuring Federated SSO and Authentication link: <https://docs.oracle.com/en/solutions/fed-ssso-options-cloud-customers/understand-federated-ssso-oracle-cloud-saas1.html#GUID-B98D5985-750D-4D66-A5E2-BCF8D4D4AD02>

Customer responsibility related to using federation is described as follows:

- When using your own identity provider, it is your responsibility to meet and maintain all PCI DSS account and password management requirements using your in-house authentication and authorization solution. Your in-house authentication and authorization mechanisms must also support the multi-factor authentication for administrative activities in the Payments module.

Shared Accounts

You should not use generic or shared accounts. You must disable the following:

- Group accounts
- Shared passwords

User Auditing

You must enable auditing of specific business objects and attributes in Payments to monitor user activity and data changes. Auditing includes recording and retrieving information pertaining to the creation, modification, or removal of business objects. Audit history records all actions that the user performs on an audited business object and its attributes. Use audit history to view changes to the application data such as the business objects that were created, updated, and deleted.

To enable auditing on Payments business objects, navigate to: Setup and Maintenance > Search Tasks: Manage Audit Policies > Manage Audit Policies page > Configure Business Object Attributes button > Configure Business Object Attributes page > Application choice list: Payables.

You must enable user auditing for the users with Financial Application Administrator or equivalent role that are responsible for Fusion Payments implementation. You must also enable auditing for users that can create or update credit cards and perform authorizations, settlements, or credit.

For information on security and assigning roles, see Oracle Database Enterprise User Security Administrator's Guide and Oracle® Financials Cloud Security Reference.

Logging

Oracle Fusion Cloud Service on OCI Payments module logs only truncated PAN values in its debug log files and never reveals more than four digits of the number, regardless of the system mask settings. No capability exists to capture the entire PAN in either diagnostics or logging files.

Oracle Fusion Payments also never logs sensitive setup values, such as keys or account profile names, except in entirely truncated format. No capability exists to write the entire setup value in diagnostics or logging files.

Oracle Fusion Payments also never logs passwords, personally identifiable information (PII) or other sensitive data.

Infrastructure

Network

The network implementation for Oracle Fusion Cloud Service on OCI relates to both internal and external communication. It is certified as PCI DSS compliant for the assessed scope as defined in the attestation of compliance (AOC). You must ensure that the network through which you access Oracle Fusion Cloud Service on OCI does not violate any PCI DSS requirements.

Wireless

Oracle Fusion Cloud Service on OCI allows, but does not require, the use of wireless network technology to access its services and functions. Using wireless communication links in your integration with Oracle Fusion Cloud Service on OCI may introduce several additional PCI DSS requirements. Consult with your PCI DSS QSA about the wireless requirements that are relevant to your environment and deployment.

Ensure that any wireless communication points in your system meet current PCI DSS requirements with respect to protocol security, key strength, periodic key rotation, key access control, and hardware-based restriction requirements.

Maintenance

Security Alerts

You must correctly implement, in a timely manner, all security alerts that you receive from Oracle. Since security alerts can affect the interaction of the Oracle Fusion Cloud Service on OCI system with your own non-Oracle applications, you must perform the required updates to remain in compliance with PCI DSS requirements.

Providing Diagnostic Information

When you need to provide log or debugging files to Oracle Support for resolving an installation issue, you may share files that contain truncated representations of PCI data. No special procedures are required to transmit such data to Oracle Support. However, you must ensure that you follow all Oracle Support policies with regard to the secure, auditable, and retention time-limited handling of your system data.

Implementation Steps

Every payment gateway provides a portal where merchants can configure their profile for the purpose of enabling credit card transactions with that payment gateway.

Merchants may configure multiple profiles where each business unit can use a separate profile for creating tokens and performing transactions.

As an example, the CyberSource configuration is described in this document. You can follow similar steps to configure any other payment gateways that may be supported in future.

Setup in CyberSource

You must have the Financial Application Administrator or an equivalent role to perform setup in CyberSource Live or Test Business Center. Use the same setup information when configuring CyberSource connectivity in Oracle Fusion Payments module.

The Financial Application Administrator role is the only ready-to-use role to perform configuration changes to Financials, including setup in Payments for tokenization. At a minimum, this role must be protected by a multi-factor authentication (MFA) mechanism for access as a privileged account that can perform administrative activities. If you create additional roles that have administrative functions, it is your responsibility to verify with your QSA if those roles and the activities they perform also require MFA access controls.

Before implementing any credit card acceptance feature in Oracle Fusion Cloud Service on OCI Payments Module, you must first have an active CyberSource merchant account and be able to access the CyberSource Business Center portal. The only ready-to-use tokenization provider supported by Oracle Fusion Payments is CyberSource. When you set up your CyberSource Merchant and Secure Acceptance accounts, you copy the setup values generated by CyberSource into the Oracle Fusion Payments setup UI.

The CyberSource Live or Test Business Center setup requirements for each Oracle Fusion Cloud Service on OCI credit card flow using the Payments module are as follows:

- **Payment Card Capture:** CyberSource Merchant account and Secure Acceptance Web/Mobile Profile account
- **Payment Card and Authorization File-Based Data Import:** CyberSource Merchant account
- **Payment Card Processing:** CyberSource Merchant account and Transaction Security key
- **Web Services:** CyberSource Merchant account

When setting up your CyberSource Merchant and Secure Acceptance accounts, ensure that your settings meet PCI DSS, territory or market, and Oracle Fusion Cloud Service on OCI requirements as follows:

CyberSource Merchant Account

- Ensure that your card security code and Address Verification Security (AVS) settings are appropriate for your territory/market and your active Oracle Fusion Cloud Service on OCI flows.
- Ensure that the token format chosen for the CyberSource merchant account is numeric and its length is less than 30-digits.

To setup CyberSource Secure Acceptance Profile and Transaction Security Key, perform the following actions in CyberSource's production or test environment:

CyberSource Secure Acceptance Profile

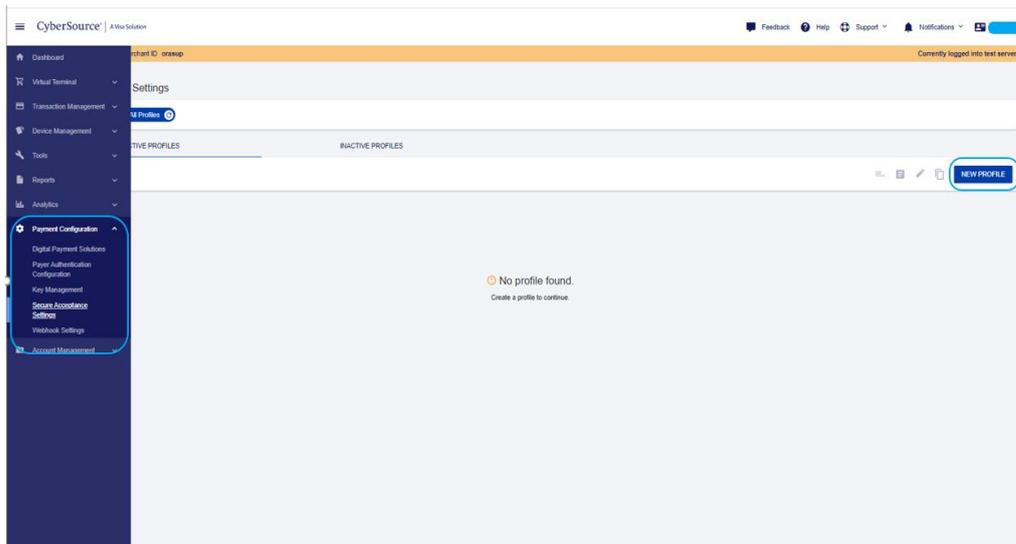
1. Sign in to the CyberSource Test Business Portal using the URL and credentials provided by CyberSource.
<https://ebctest.CyberSource.com/ebctest> or <https://ubctest.CyberSource.com/ebc2>

To sign in, you need the following details from CyberSource:

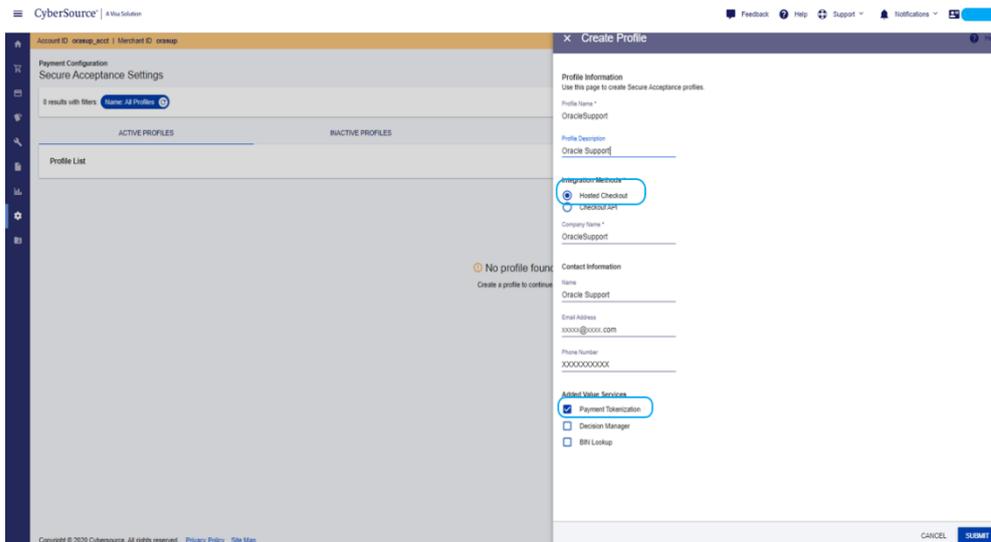
Property	Value
CyberSource Merchant ID	<Organization ID>
Username	<Username>
Password	<Password>

2. Create a Secure Acceptance Profile

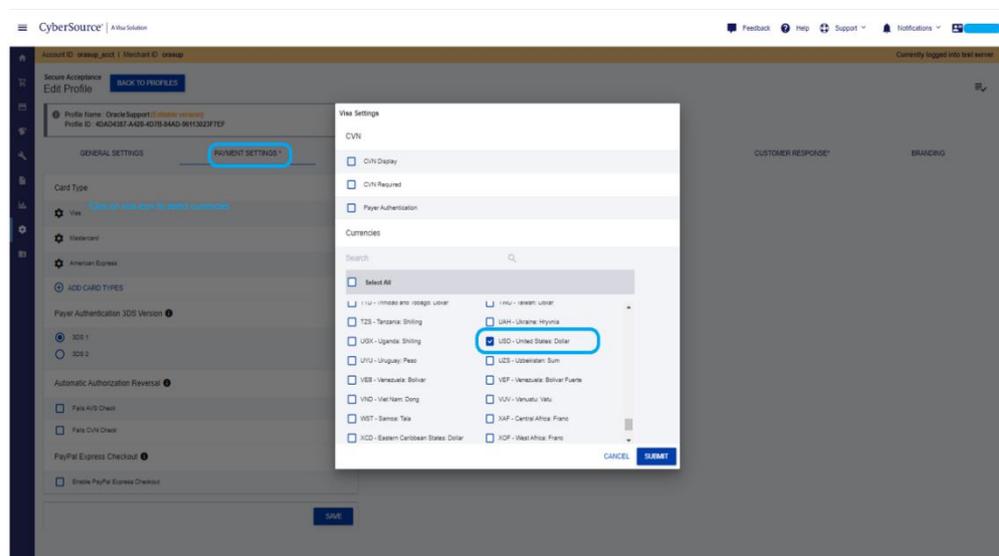
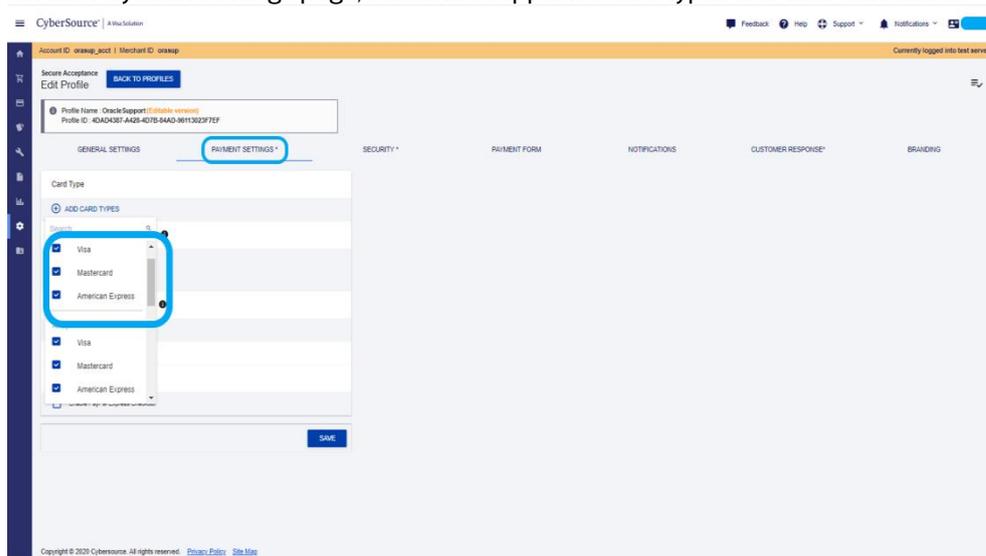
- a. Go to Tools & Settings > Secure Acceptance > Profiles. Click the **New Profile** button.



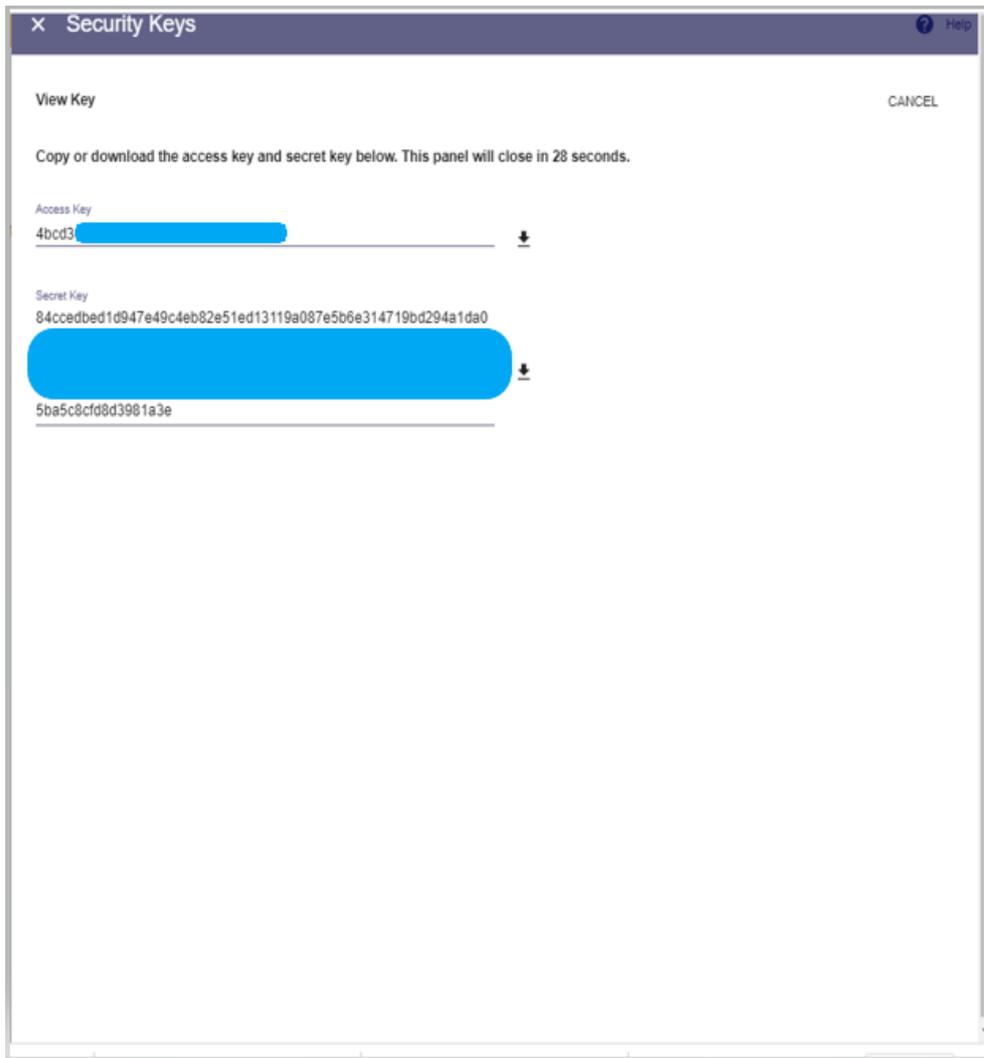
- b. Under General Settings, select the following options:



- c. On the Payment Settings page, select the supported card types and their currencies.

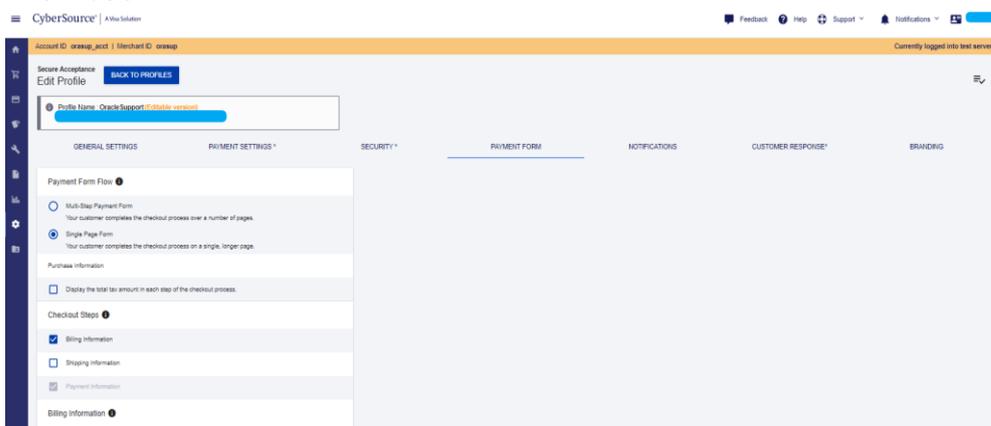


- d. On the Security page, Click **Generate** to generate secure acceptance keys.
- e. Enter the key name, signature version, and signature method ((as HMAC-SHA256) and click **Create**. This generates and displays the Secure Acceptance Access Key and the Secret Key as shown in the following:

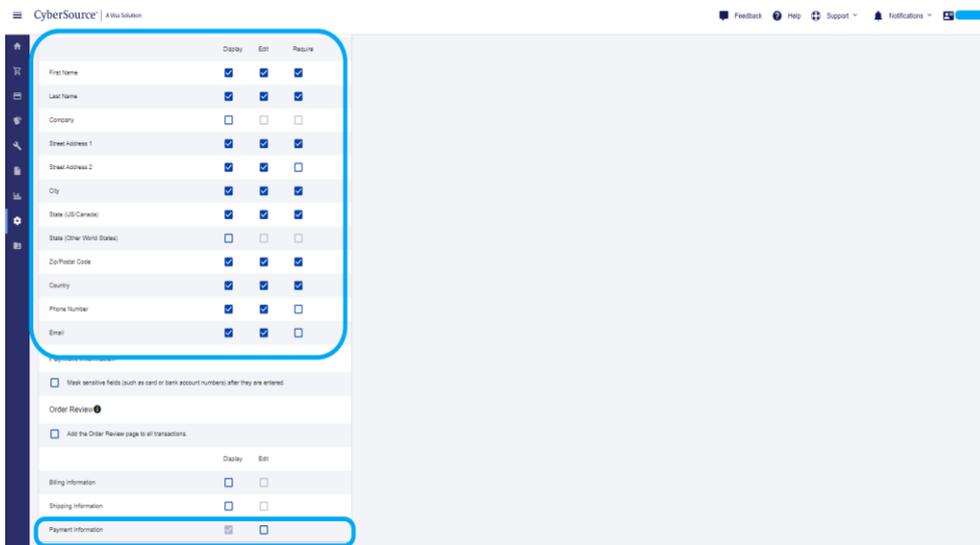


Make sure to download and safely store both keys as they are required for performing Payments setup.

- f. Navigate to the Payment Form page and select the following options for **Single Form** and **Billing Information**:



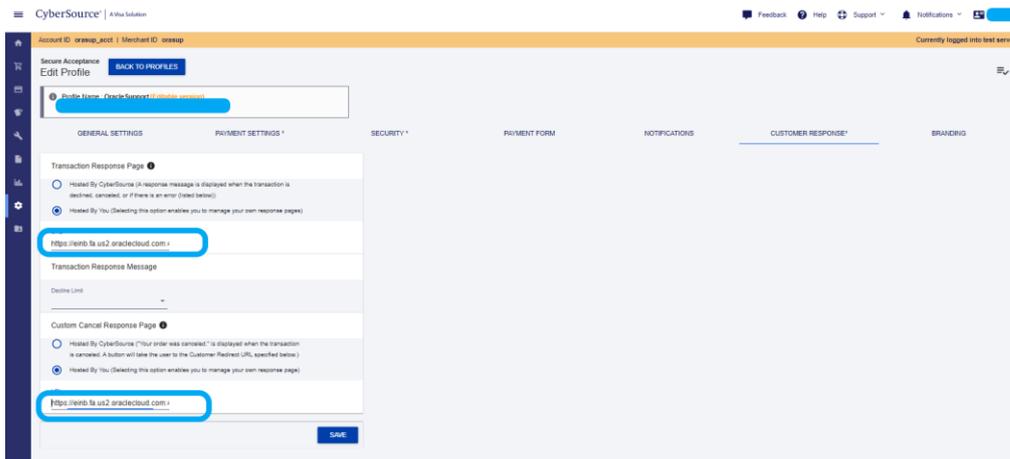
- g. Select the billing options based on your address verification requirements. Some of these fields may be mandatory for the hosted service. Consult CyberSource documentation for further guidance.



Note: The billing selections shown here are only for example.

- h. Navigate to the Customer Response page and select the **Hosted By You** option for both the transaction response and custom cancel response. Enter the response URL in the following format:
<https://<host.domain:port>/fscmUI/faces/adf.task-flow?adf.tfId=AuthorizationHostedReturnFlow&adf.tfDoc=/WEB-INF/oracle/apps/financials/payments/fundsCapture/transactions/ui/flow/AuthorizationHostedReturnFlow.xml>

Note: Replace <host.domain:port> with values for your SaaS POD.



- i. Note down the Secure Acceptance Profile ID and save the profile.

Securely copy the data from the applicable CyberSource fields of your Secure Acceptance Web/Mobile Profile account and paste the data as follows:

- Paste the Token Client Identifier into the Value field for the Client Identifier setting on the Edit Payment System: CyberSource page.
- Paste the Secure Acceptance Access Key into the Value field for the Secure Acceptance Access Key setting on the Edit Payment System: CyberSource page.
- Paste the Secure Acceptance Signature Key into the Value field for the Secure Acceptance Signature Key setting on the Edit Payment System: CyberSource page.

Note: Ensure that you differentiate between test and production profile values. Enter the appropriate values, depending on your Oracle Fusion Cloud Service on OCI system.

Transaction Security Key

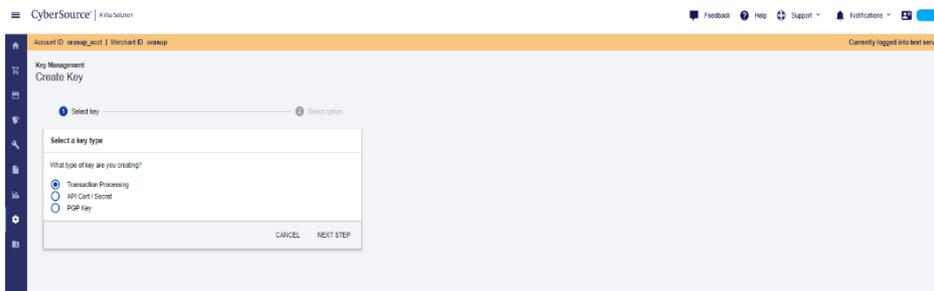
To generate the Transaction Security Key, navigate as follows in CyberSource:

**15 Business / Technical Brief / Oracle Fusion Cloud Service on OCI Payments Module
 PCI DSS Implementation / Version 1.9**

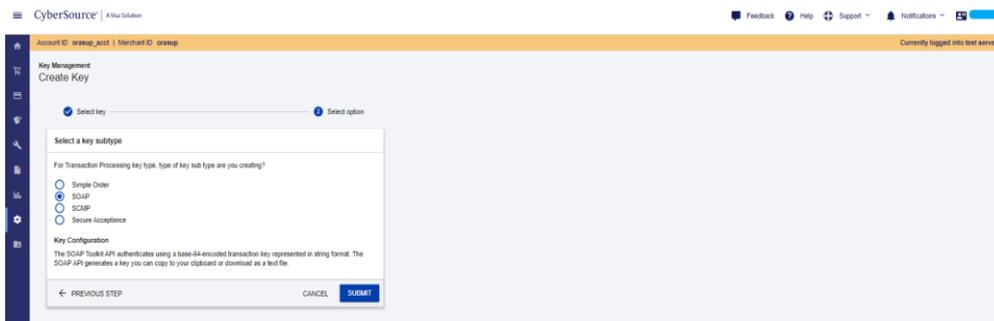


Payment Configuration → Key Management → Generate Key

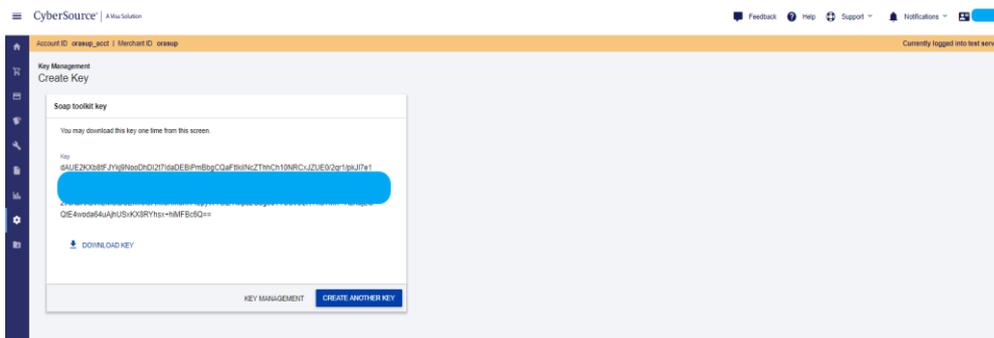
1. Select Transaction Processing and click Next Step.



2. For the key sub type, select **SOAP** and then submit.



3. Click **Download Key** to download and store the SOAP Toolkit key safely.

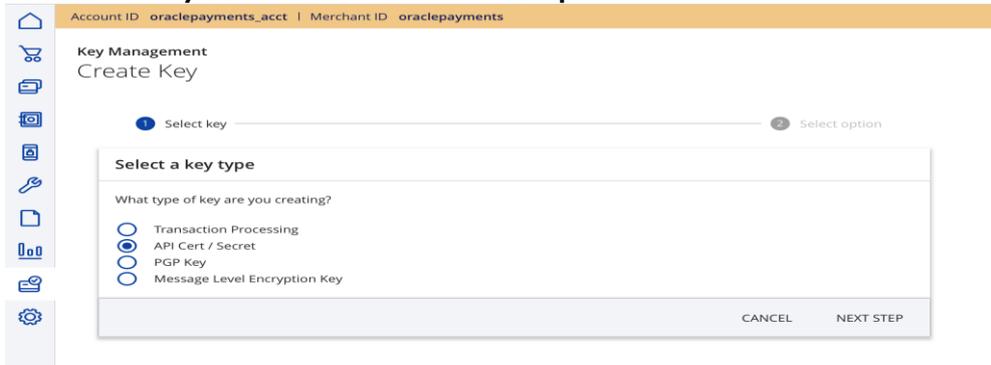


Shared Secret Key

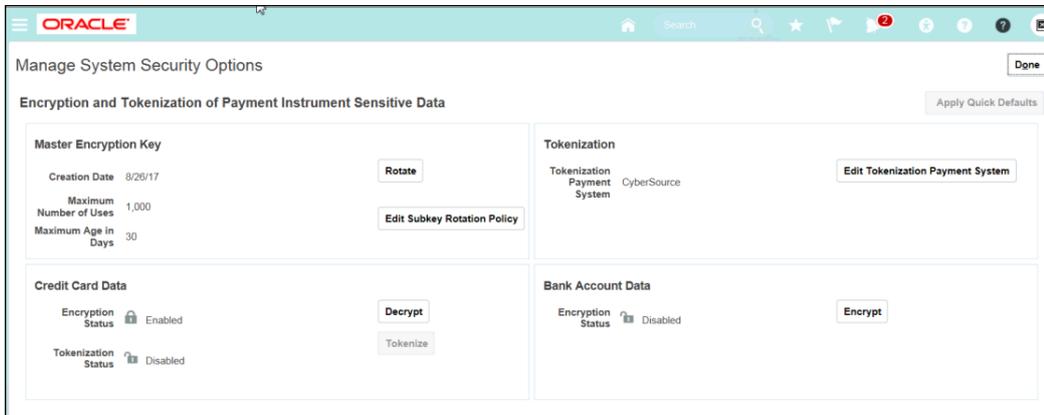
To generate the Shared Secret Key, navigate as follows in CyberSource:

Payment Configuration → Key Management → Generate Key

1. Select **API Cert / Secret** and then click **Next Step**.



2. In the Setup and Maintenance work area, go to the **Manage System Security Options** task:
 - Offering: Financials
 - Functional Area: Payments
 - Task: Manage System Security Options



Setting up security options

Note: Before you can enable tokenization for credit cards or encryption for bank account data, you must create a system key. The system key resides in the OPSS secure repository. The application uses your system key to encrypt your sensitive data.

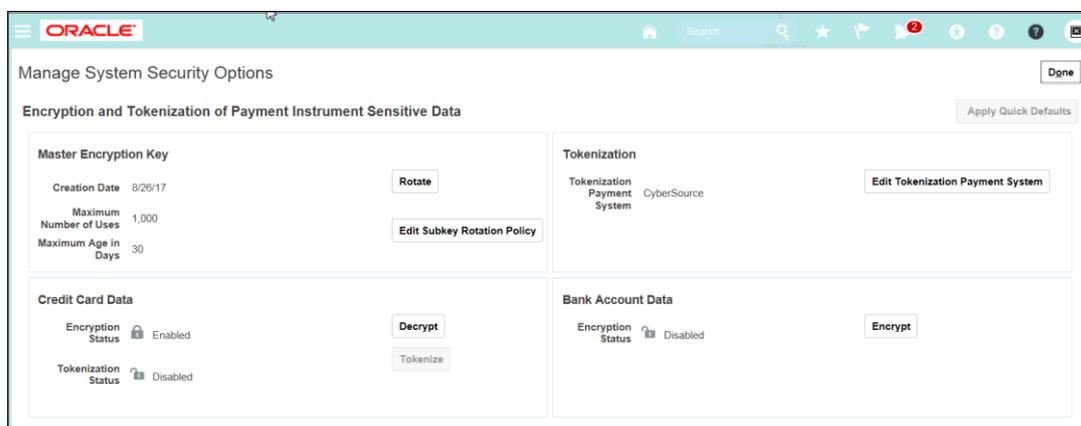
- To create a system key, see the steps 1 to 3 in the Tokenization Setup section in this document.
- To enable tokenization for credit card data, click **Tokenize**.
- To encrypt bank account data, click **Encrypt**.

If you tokenize your credit card data, you are complying with PCI DSS requirements. Oracle Fusion Payments only supports credit card services in an environment where you enable tokenization.

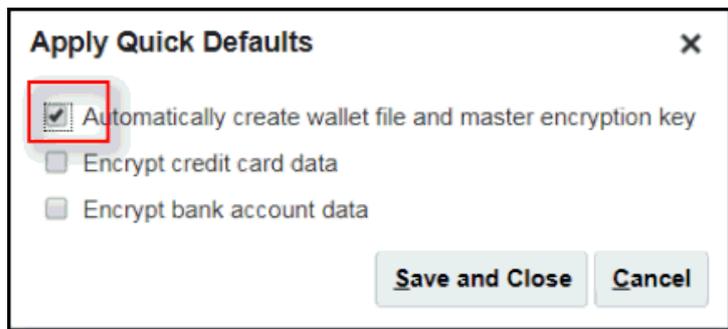
Tokenization is the process of replacing a payment card PAN with a unique number (or token) that is not sensitive. CyberSource acts as a third-party payment system and stores the sensitive information and generates tokens that replace sensitive data in the application and the database. Unlike encryption, tokens cannot be reversed or used to mathematically derive the actual credit card PAN.

Before you can set up tokenization, you must create a master encryption key. To create a master encryption key, follow these steps:

1. On the Manage System Security Options page, click **Apply Quick Defaults**.



2. In the Apply Quick Defaults dialog box, select Automatically create wallet file and master encryption key.



3. Click **Save and Close**.

Note: After you create the wallet file for the first time, the Apply Quick Defaults button is disabled.

For enabling credit card feature for your environment, follow these steps:

1. Submit a services request with the following details to receive a cryptographic key from Oracle. This key is specific to the environment mentioned in the service request. The key is used for validating that the customer's environment is eligible for credit card processing:
 - Product: Fusion Payments Cloud Service
 - Subject: <POD Name>: Generate Key for Enabling Credit Card Feature using Lookup
2. Create a lookup using the following details:
 - Lookup Type: IBY_TIME_BOUND_SWITCH
 - Lookup Type Meaning: Time bound switch to enable credit card feature
 - Lookup Type Description: Time bound switch to enable credit card feature
 - Module: Payments
 - Lookup Code: IBY
 - Meaning: Temporary (Time-bound) Secret Key Shared by Oracle
 - Description: Temporary (Time-bound) Secret Key Shared by Oracle
 - Enabled: (Selected)
3. Navigate to Scheduled Processes and search for **Import Security Credential Job**. The Credential File Type drop-down now displays a new option **Enable Credit Card Feature**. Select this option to run the ESS job. Credit card feature should get enabled on the POD once this job completes successfully.

Process Details ✕

i This process will be queued up for submission at position 1

Process Options Advanced Submit Cancel

Name Import Security Credential Job

Description Imports security-related credential files, such... Notify me when this process ends

Schedule As soon as possible **Submission Notes**

Basic Options

Parameters

Retrieval Transmission Configuration

Credential File Type Enable Credit Card Feature

Security Credential Name

UCM File Name

4. A new lookup code is predefined to allow this feature to be enabled or disabled. Details are as follows:

- Lookup Type: ORA_IBY_CONTROLLED_FEATURES
- Lookup Code: IBY_FEATURE_GEN_ARCH

This feature is currently disabled by default. Add and enable the above lookup code to enable the feature.

Note: You must raise separate service requests and perform these steps for each of your development, test, and production environments because the key issued by Oracle is separate for each environment and cannot be used for a different environment.

Tokenization Setup

Check the Tokenization Status in the Credit Card Data section on the Manage System Security Options page. If the Tokenization Status is Disabled, then complete the Oracle Fusion Payments setup to enable credit card tokenization.

The screenshot shows the Oracle Manage System Security Options page. The main section is titled "Encryption and Tokenization of Payment Instrument Sensitive Data". It is divided into four panels:

- Master Encryption Key:** Shows creation date (8/26/17), maximum number of uses (1,000), and maximum age in days (30). Buttons for "Rotate" and "Edit Subkey Rotation Policy" are present.
- Tokenization:** Shows "Tokenization Payment System" set to "CyberSource" with an "Edit Tokenization Payment System" button.
- Credit Card Data:** Shows "Encryption Status" as "Enabled" and "Tokenization Status" as "Disabled". Buttons for "Decrypt" and "Tokenize" are present.
- Bank Account Data:** Shows "Encryption Status" as "Disabled" with an "Encrypt" button.

To configure Oracle Fusion Payments integration with CyberSource, perform the following tasks in Oracle Public Cloud Applications.

Prerequisites:

- You have already completed the CyberSource secure acceptance profile setup described earlier in the document.
- You have set up a Payments Administration user with multi-factor authentication using a compliant identity management solution. This user must perform all the setups described for tokenization.

Tokenization setup in Oracle Fusion Payments consists of the following tasks:

- Payment System and Payment System Account
- Transmission Configuration
- Funds Capture Process Profile
- Payee
- Payee Routing Rules
- System Security Options

Payment System Setup

1. Sign into the Oracle Fusion SaaS Cloud Applications.
2. Click **Navigator > My Enterprise > Setup and Maintenance**.
3. In the Setup and Maintenance work area, go to the **Manage Payment System** task:
 - Offering: Financials
 - Functional Area: Payments
 - Task: Manage Payment System
4. On the Manage Payment Systems page, enter **CyberSource** in the **Name** field.
5. Click **Search**.
6. In the Search Results section, click the CyberSource link.
7. On the Edit Payment System page, you must select the following options for supported capabilities, tokenization, formats, and transmission configuration:

The screenshot displays the 'Edit Payment System' configuration page for CyberSource. The top section contains fields for Name (CyberSource), Code (cys), Processing Model (Gateway), Bank, and Network Communication Character Set. Below this are fields for Transmission Serial Base URL, Administrative URL, From Date (10/17/12), and To Date (mm/yy). The 'Supported Capabilities' section includes checkboxes for Funds Capt... (Credit card, Electronic funds transfer, Debit card), Disburse... (Electronic funds transfer and positive pay), and Tokenization Payment System Sett... (Credit card tokenization). The 'Form...' section shows a list of items with 'HTML POST Request' selected. The 'Transmission Proto...' section also shows 'HTML POST Request' selected.

8. Securely copy values from your CyberSource merchant account and your Secure Acceptance profile. Enter them in the Value fields in the Tokenization Payment System Settings section on the Edit Payment System: CyberSource page for the following settings:

Tokenization Payment System Settings ②

View ▾ + × Freeze ↵ Wrap

* Name	* Code	* Data Type	Secured	* Value
SOAP API Security Key	SOAP_UPG_SEC_KEY	VARCHAR2	Y	*****
Secure Acceptance Access Key	ACCESS_KEY	VARCHAR2	Y	*****
Secure Acceptance Signature Key	SIG_KEY	VARCHAR2	Y	*****
Tokenization Servlet Base URL	TOKEN_CREATE_URL	VARCHAR2	N	https://testsecureacceptance.cybersource.c
Tokenization Payment URL	TOKEN_PAY_URL	VARCHAR2	N	https://testsecureacceptance.cybersource.c
Client Identifier	TOKEN_CREATE_CLIENT	VARCHAR2	Y	*****
Token Creation Module	TOKEN_CREATE_HANDLER	VARCHAR2	N	CyberSource Secure Acceptance Web ▾
Tokenization Upgrade URL	TOKEN_UPGRADE_URL	VARCHAR2	N	https://cs2wstest.ic3.com:443/commerce/1
Upgrade Client Identifier	TOKEN_UPGRADE_CLIENT	VARCHAR2	Y	*****
Token Upgrade Module	TOKEN_UPGRADE_HANDLER	VARCHAR2	N	Tokenization Upgrade Disabled ▾
Key Identifier for Card Security Code and Transaction...	MICROFORM_KEY_ID	VARCHAR2	N	17e7b6b5-d00a-4264-af0e-9a41fd2af27b
Shared Secret Key for Card Security Code and Transa...	MICROFORM_SHARED_SEC_KEY	VARCHAR2	N	2C7+EcvotqBbdK0NwouJ5UE0lOg696Df
Credit Card Token Request Response Format	TOKEN_RESPONSE_FORMAT	VARCHAR2	N	CyberSource Card Tokenization Request ▾
Signing Algorithm	SIGNATURE_ALGORITHM	VARCHAR2	N	HMAC-SHA256 ▾
Merchant Account for Card Security Code and Transa...	MICROFORM_MERCHANT_ID	VARCHAR2	N	oraclepayments
Create URL for Card Security Code	MICROFORM_CREATE_URL	VARCHAR2	N	https://apitest.cybersource.com/flexv1/keys
Credit Card Token Request Format	TOKEN_REQUEST_FORMAT	VARCHAR2	N	CyberSource Card Tokenization Request ▾

Note: If your Oracle Fusion Cloud Service on OCI instance is a test environment, ensure that you copy these values from your test CyberSource account. If you are using the Oracle Fusion Cloud Service on OCI production environment, ensure that you copy these values from your production CyberSource account:

- **Tokenization Servlet Base URL (TOKEN_CREATE_URL code):** The CyberSource Secure Acceptance Web/Mobile token that creates an URL endpoint. The URL is a constant value.
 - The [Secure Acceptance Hosted Checkout Guide](#) provides the URL.
- **Tokenization Payment URL (TOKEN_PAY_URL code):** The CyberSource Secure Acceptance Web/Mobile payment token (tokenization + authorization) that creates an URL endpoint.
 - The [Secure Acceptance Hosted Checkout Guide](#) provides the URL.
- **Client Identifier (TOKEN_CREATE_CLIENT code):** The CyberSource Secure Acceptance profile identifier.
 - The CyberSource Business Center provides this code after you set up a Secure Acceptance profile.
- **Token Creation Module (TOKEN_CREATE_HANDLER code):**
 - From the Value choice list, select **CyberSource Secure Acceptance Web**.
- **Secure Acceptance Access Key (ACCESS_KEY code):** The Secure Acceptance Access Key.
 - The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **Secure Acceptance Signature Key (SIG_KEY code):** The Secure Acceptance Signature Key.
 - The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **MICROFORM_MERCHANT_ID**

- The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **MICROFORM_KEY_ID**
 - The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **MICROFORM_SHARED_SEC_KEY**
 - The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **TRANSACTION_SEARCH_URL**
 - The CyberSource Business Center provides this code after you set up the Security module in your Secure Acceptance profile.
- **MICROFORM_CREATE_URL**
 - Customers need to work with CyberSource to get the URL value

Leave the other Value fields empty. For questions on URL values for TEST and PRODUCTION accounts, refer to the following table and consult CyberSource.

Name	Code	Cybersource Field	Value
SOAP API Security Key	SOAP_UPG_SEC_KEY	SOAP Toolkit Key	ZnWz8Wts+DrPIQsLY3RoKFjyufqzDToTKC/BKUQWUBldCHsNuELcbG3Y07aA61ApZ9jVajjJX68Vv54NmEDPFY11Yv1UB2MAQjAwobwrr//khQruHVjilsYluohbzAwYrqk9cSgYXWz91kIqtuZQ074na/QpFhSj5m+414OW
Secure Acceptance Access Key	ACCESS_KEY	Secure Acceptance Access Key	4bcd36d094ab3bb6b09a7becefb1e8b6
Secure Acceptance Signature Key	SIG_KEY	Secure Acceptance Secret Key	84ccedbed1d947e49c4eb82e51ed13119a087e5b6e314719bd294a1da031ab8d6de86953053c40dfafef5ed39978ada6b99820060aa48e38f999a9b7d943ab0515de5f081b94b269ec36b87d5871681a8fc433298d4099866
Client Identifier	TOKEN_CREATE_CLIENT	Secure Acceptance Profile ID	4DAD4387-A428-4D78-84AD-96113023F7EF
Tokenization Servlet Base URL	TOKEN_CREATE_URL	N/A	https://testsecureacceptance.cybersource.com:443/embedded/token/create
Tokenization Payment URL	TOKEN_PAY_URL	N/A	https://testsecureacceptance.cybersource.com:443/embedded/pay
Token Creation Module	TOKEN_CREATE_HANDLER	N/A	Cybersource Secure Acceptance Web
Tokenization Upgrade URL	TOKEN_UPGRADE_URL	N/A	https://ics2wstest.ic3.com:443/commerce/1x/transactionProcessor
Upgrade Client Identifier	TOKEN_UPGRADE_CLIENT	Merchant ID	orasup
Token Upgrade Module	TOKEN_UPGRADE_HANDLER	N/A	Tokenization Upgrade Disabled

9. Click **Save and Add Accounts**.
10. In the Payment System Accounts section, enter information in all Value fields.
11. For the Commerce Indicator setting, enter **internet** in the Value field.
12. In the Value field for the SOAP API Security Key setting, enter the same value you entered in the SOAP API Security Key field on the Edit Payment System: CyberSource page.

Name	Code	Cybersource Field	Value
Business Unit	BU_NAME	N/A	Vision Operations
Client Identifier	TOKEN_CREATE_CLIENT	Secure Acceptance Profile ID	4DAD4387-4A28-4D78-84AD-96113023F7EF
Commerce Indicator	COMMERCE_INDICATOR	N/A	Internet
Merchant City	DESCRIPTOR_CITY	N/A	Frisco
Merchant ISO Country Code	DESCRIPTOR_COUNTRY	N/A	US
Merchant Identifier	MERCHANT_ID	Merchant ID	orasup
Merchant Name	DESCRIPTOR	N/A	Leave Blank
Merchant Phone Number	DESCRIPTOR_CONTACT	N/A	407-555-1212
Merchant Postal Code	DESCRIPTOR_POSTALCODE	N/A	75035
Merchant State	DESCRIPTOR_STATE	N/A	TX
Merchant Street Address	DESCRIPTOR_STREET	N/A	1 Oracle Pkwy
Point of Sale Operating Environment	POS_ENVIRONMENT	N/A	Leave Blank
SOAP API Security Key	SOAP_UPG_SEC_KEY	SOAP Toolkit Key	ZrWZx8Wts+DrPIQsLY3RokFjyufqaZD7oTxc/BKUCQWUBi0cHsNuEJLccg3Y07a61ApZ9jVayjUX68Vv54NmEDPF11YV1UB2MAQAwobwrr/JkrQruHvjIlsYluobzAwwYrkt9cSgYXWz91rklqtuZQj074na/QpPhSs5m+4s
Secure Acceptance Access Key	ACCESS_KEY	Secure Acceptance Access Key	4bcc36d094ab3bb6b09a7bece81e8b6
Secure Acceptance Signature Key	SIG_KEY	Secure Acceptance Secret Key	84ccedbed1d947e49c4eb82e51ed13119a07e5b6e314719bd294a1da031ab8d6de86953053c40d9f9ef5ec39978ada6b99820060aa48e38P999a9b7d943ab0515de5D81b94b269ec36b87d5871681a8fc433296d409
Token Creation Currency	ACCT_TOKEN_CREATE_CURRENCY	N/a	USD

13. Click **Save and Close** to complete the payment system setup.

Transmission Configuration Setup

1. Click **Navigator > My Enterprise > Setup and Maintenance**.
2. In the Setup and Maintenance work area, go to the **Manage Transmission Configurations** task:
 - Offering: Financials
 - Functional Area: Payments
 - Task: Manage Transmission Configurations
3. From the **Select Protocol** drop-down list, select **HTTP(s) Post Request** protocol and then click **Create**.

4. Enter the following details:

ORACLE

Edit Transmission Configuration: CYS SOAP Test Center

* Configuration: CYS SOAP Test Center

Protocol: Http(s) POST Request

Tunneling Configuration: [v]

Parameters

View [v] [Freeze] [Wrap]

Name	Data Type	Value
*Destination URL	Character	https://ics2vrstest.ic3.com/commerce/1.x/transactionProcessor
HTTP Authentication User Name	Character	
HTTP Authentication Password	Character	
Proxy Host	Character	
No Proxy Domain	Character	
Wallet Location	Character	
Wallet Password	Character	
*Send Body Content Type	Character	text/xml
*Receive Body Content Type	Character	text/xml
Ignore Response	Character	
PGP Public Encryption Key	Character	
PGP Private Signing Key	Character	
PGP Private Key Password	Character	

5. Click **Save and Close**.

Funds Capture Process Profile Setup

1. Click **Navigator > My Enterprise > Setup and Maintenance**.
2. In the Setup and Maintenance work area, go to the **Manage Funds Capture Process Profiles** task:
 - Offering: Financials
 - Functional Area: Customer Payments
 - Task: Manage Funds Capture Process Profiles.
3. Under **Select Processing Type** drop-down, select **Credit card** and then click **Create**.
4. Enter the following details:
 - Processing Type = Credit Card
 - Name = Unique Name
 - Code = Unique Code
 - Payment System = CyberSource
5. Click on the **Formats** tab and select the formats as shown in the following:

Edit Funds Capture Process Profile ? Save Save and Close Cancel

Processing Type: Credit Card

* Name: CyberSource SOAP Toolkit 1.86

Code: ORA_CYS_SOAP_1_86

Payment System: CyberSource

Use for external settlement

Description:

* From Date: 3/7/13

To Date: m/d/yy

Formats | Settlement Batch | Accounts | Additional Information

Authorization

* Outbound Format: CyberSource Transaction Request

* Inbound Response Format: CyberSource Settlement Response

Settlement ?

* Outbound Format: CyberSource Transaction Request

Inbound Response Format: CyberSource Settlement Response

Settlement Response Processing

Outbound Format: CyberSource Transaction Request

Inbound Response Format: CyberSource Settlement Response

Notification to Payer

Format: Receipt of Payment Notification Format

Delivery Method: E-Mail

Override payer delivery method preference

6. Click on the Settlement Batch tab and specify creation rules or limits as per your requirements. These are optional details.

Note: Leave the Settlement Batch Directory field blank. This is not relevant for SaaS deployments.

7. Click on the Accounts tab and specify the transmission configuration details for authorization and settlement as shown in the following:

ORACLE ORACLE Home Star Refresh Notifications TS

Create Funds Capture Process Profile Save Save and Close Cancel

Processing Type: Credit Card

* Name: ORASUP_FCFF

* Code: ORASUP_FCFF

* Payment System: CyberSource

Description:

* From Date: 4/22/09

To Date: m/d/yy

Formats | Settlement Batch | **Accounts** | Additional Information

View ▼ Focus Wrap

Payment System Account	Configuration Profile	Transmission Configuration			From Date	To Date
		Authorization	Settlement	Acknowledgmen		
orasp	ORASUP_FCFF orasp	CYS SOAP Tr	CYS SOAP Tr	CYS SOAP Tr	3/2/09	m/d/yy
oracpayments	ORASUP_FCFF oracpayments	CYS SOAP Tr	CYS SOAP Tr	CYS SOAP Tr	4/22/09	m/d/yy

8. Click **Save and Close**.

Internal Payee Setup

1. Click **Navigator > My Enterprise > Setup and Maintenance**.

2. In the Setup and Maintenance work area, go to the **Manage Internal Payees** task:

- Offering: Financials
- Functional Area: Customer Payments
- Task: Manage Internal Payees.

3. Click on the **Create** icon to create a new payee as shown in the following:

4. Associate the payment system, the payment system account, and the business unit with the payee.

Note: A business unit can only be assigned to one payee.

5. Click **Save and Close**.

Payee Routing Rule Setup

This is an optional setup required only in case of multiple business units, CyberSource accounts, and so on, to ensure that payments are routed to the correct CyberSource merchant ID (MID) and profile. For a simple setup with just one business unit, one CyberSource MID and profile, no routing is required. To create a routing rule, select the payee and click **Manage Routing Rule**:

Payee	Code	Merchant Category Code
EDBPayee	EDB_Payee_Code	
AHL_Payee	1235	
VSL_Payee	VSL_Payee_Code	
ORASUP Payee	ORASUP_PVYEE	

The Manage Routing Rules page has default routing rules which apply when no routing rule is specified, or when none of the routing rule conditions were met.

On the same page, you can also define the routing rules with specific conditions and routing rules.

Priority	Routing Rule Name	Payment Method	Payment System	Funds Capture Process Profile	Status
1	cysr-10000	Credit Card	oraspayments	CyberSource SQAP Toolkit 1.00 oraspayments	Active
2	EDB_Routing_Name	Credit Card	EDBPS_Account	EDB_FCPP EDBPS_Account	Active
3	cysr1-1000	Credit Card	orasp	ORASUP_FCPP orasp	Active

To create a routing rule, follow these steps:

1. Select **Credit Card** as payment method and then click **Create**.

- Enter the following details to create a routing rule that sends any payment with amount between \$501-\$1000 to CyberSource 'orasup' MID.

You can see the following attributes in the Criterion drop-down list to create the routing rule condition:

- Amount
- Business unit
- Card brand
- Card number
- Currency
- Factored receipt
- Payee bank
- Payee bank account
- Payee bank country
- Receivables receipt method

Note: Not all attributes are applicable to Credit Card payment method.

- Click **Save and Close**.

System Security Option Setup

This last step is required to enable tokenization with CyberSource as tokenization service provider.

Prerequisite: Create wallet

Note: If the wallet is already created, the Apply Quick Defaults button is disabled.

- In the Setup and Maintenance work area, go to the **Manage System Security Options** task:
 - Offering: Financials
 - Functional Area: Customer Payments
 - Task: Manage System Security Options
- Click **Tokenization Payment System** and select **CyberSource** as the tokenization service provider.
- Click **Tokenize** in Credit Card Data section to enable tokenization as shown in the following:

Note: If the Tokenize button is disabled, it indicates that one of the setups was incomplete or incorrect. Check to ensure that all setups are done correctly.

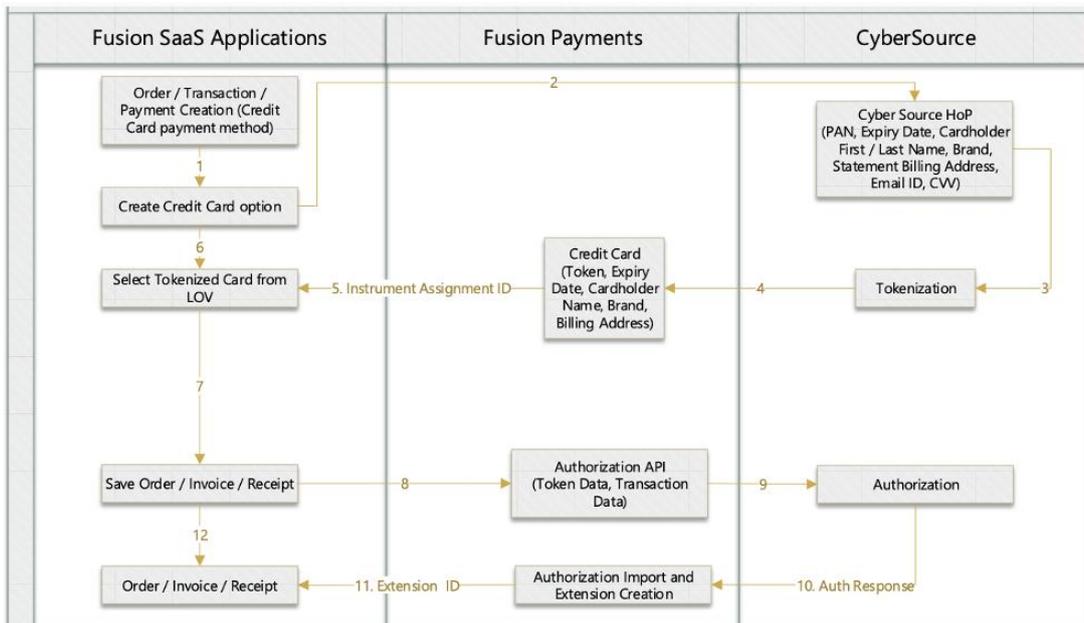
Note: Whenever an environment is refreshed using another environment, such as Production-to-Test (P2T) or Test-to-Test (T2T), perform the instructions mentioned in the document [Payments Wallet Migration Post P2T / T2T Refresh \(Doc ID 2407678.1\)](#) immediately after such a refresh, before doing a new credit card creation or transaction.

This completes the Oracle Payments and CyberSource integration setup for tokenization and payment processing services. You can now create tokens and test payment processing from the Oracle Receivables application.

Credit Card Business Flows

UI Flow

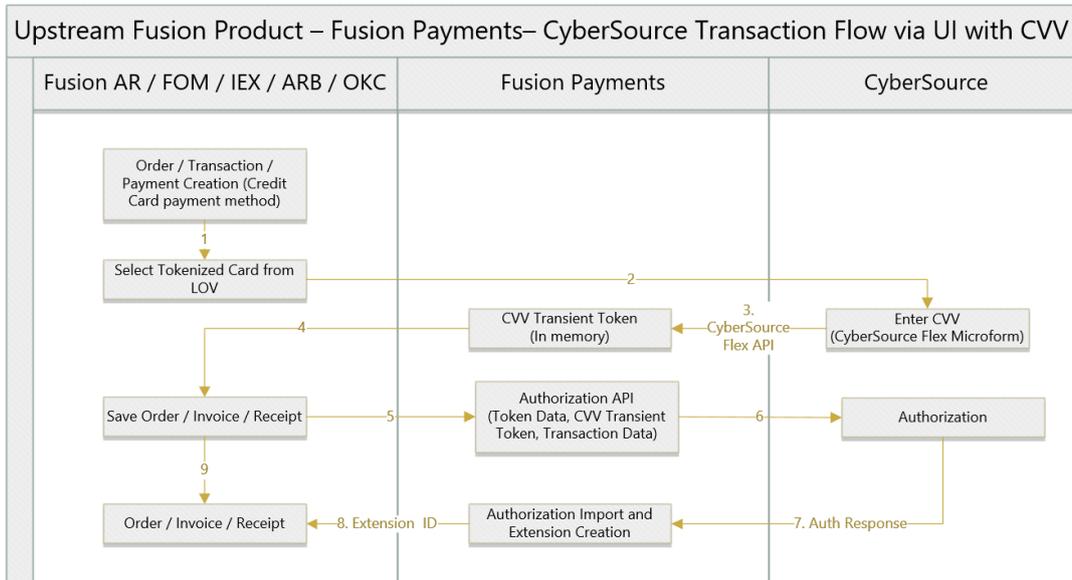
- During transaction creation flows in Oracle Fusion SaaS Applications, users get the options to specify a credit card.
- Users can choose a card that was created earlier from a list of values. The credit cards are tokenized and displayed as masked in the list.
- Alternatively, users can choose to specify a new credit card which navigates them to CyberSource’s Secure Acceptance Page.
- CyberSource stores the specified credit card and sends the tokenized card number to Oracle Fusion Payments. The tokenized number is stored along with other cardholder data such as expiry date, cardholder name, brand, and billing address.
- For credit card authorization, Oracle Fusion Payments passes the tokenized card number to CyberSource which then returns the authorization response to Oracle Fusion Payments.



UI Flow with CVV support

- The credit card security code (CVV) is securely passed to CyberSource for transactions on a saved credit card.
- In addition to the UI flow described earlier, the application renders the CyberSource CVV flex-microform field using a JWT token when the user selects a card (Card on file) from the drop-down list.
- When the user enters the CVV value to make a payment, a transient CVV token is generated and stored in-memory for the session.

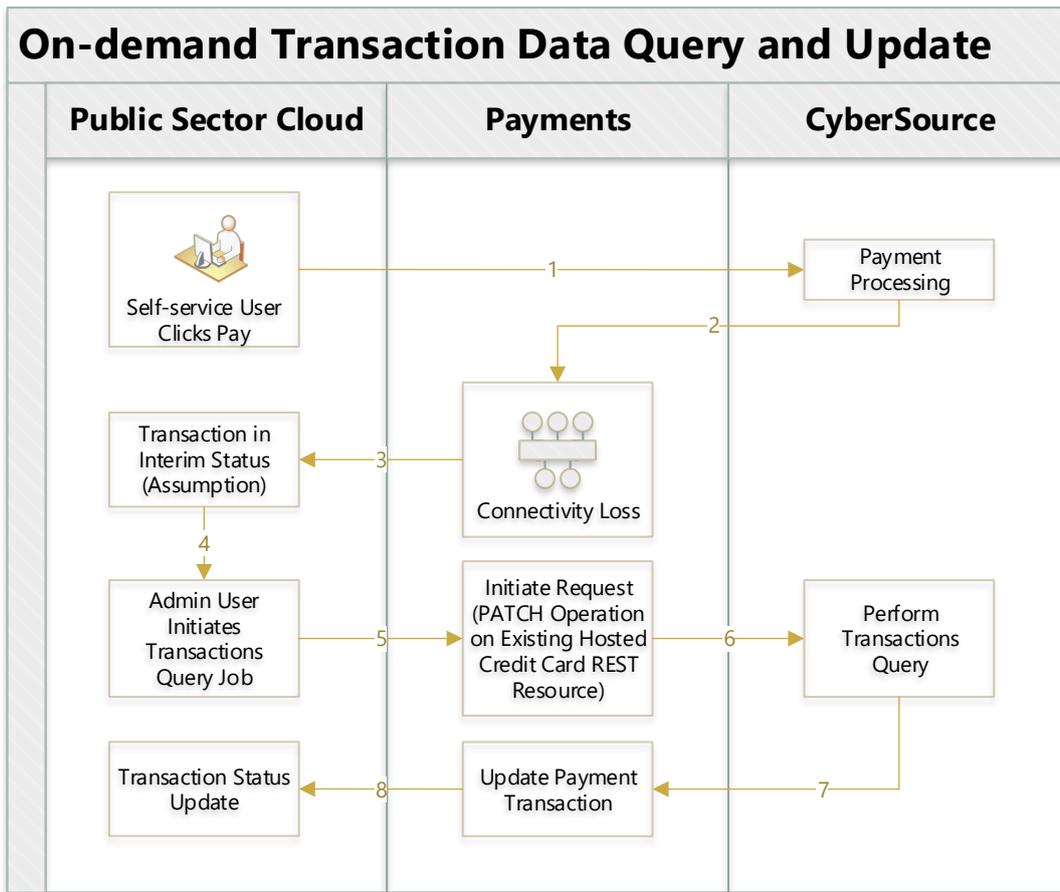
- CyberSource stores the specified credit card and returns the tokenized card number to Oracle Fusion Payments. The tokenized card number is stored along with other cardholder data such as expiry date, cardholder name, brand, and billing address.
- For credit card authorization, Oracle Fusion Payments securely passes the tokenized card number and the transient CVV token to CyberSource which then returns the authorization response to Oracle Fusion Payments.
- In this manner, the credit card security code (CVV) will be securely passed to CyberSource for saved credit card transactions.



Flow for Handling Failed or Orphaned Transactions Using CyberSource Query

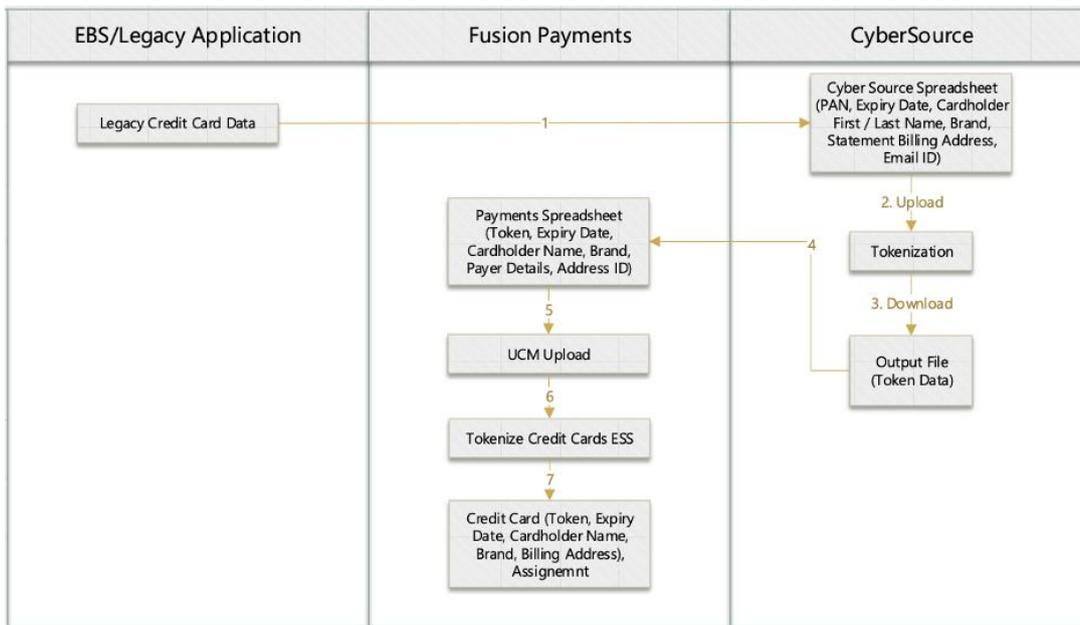
- While making payments from Oracle Public Sector Cloud, internet connectivity loss or non-recommended user actions (clicking back button or refresh on browser) may cause a data inconsistency where payment is successfully completed in CyberSource, but no response is updated in Oracle Fusion Payments and Oracle Public Sector Cloud.
- Oracle Payments provides the capability for Oracle Public Sector Cloud to initiate a request to query with CyberSource for transactions with inconsistent data.
- Oracle Payments takes the request from Oracle Public Sector Cloud, queries with CyberSource, updates the payment information with the query result, and provides payment status to Oracle Public Sector Cloud.

On-demand Transaction Data Query and Update



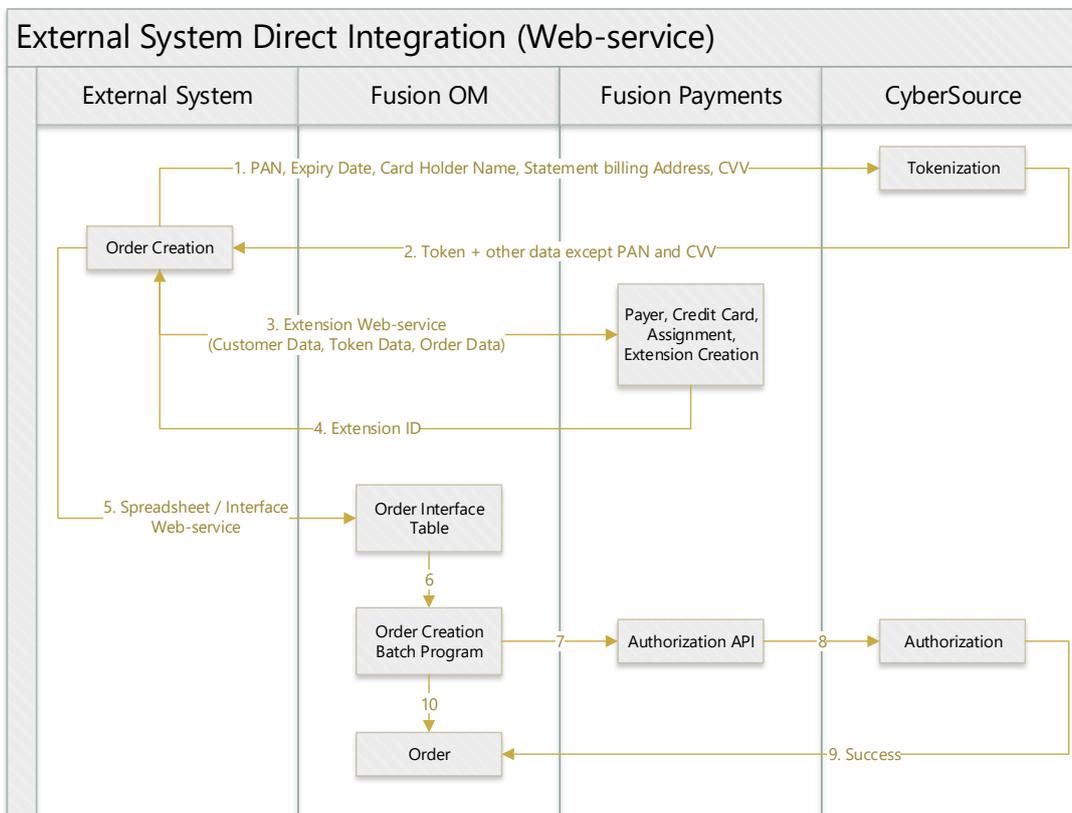
Spreadsheet Import Flow

- Oracle Fusion Payments provides the capability to interface legacy credit card data with tokenized credit card numbers.
- In this flow, the tokenized credit card number, card holder name, card brand, expiry date, billing address, and email address are first interfaced into CyberSource wherein the card number is tokenized and is returned along with other cardholder data in an output file.
- The tokenized card number, expiry date, cardholder name, card brand, and billing address are then interfaced into Oracle Fusion Payments using a spreadsheet.



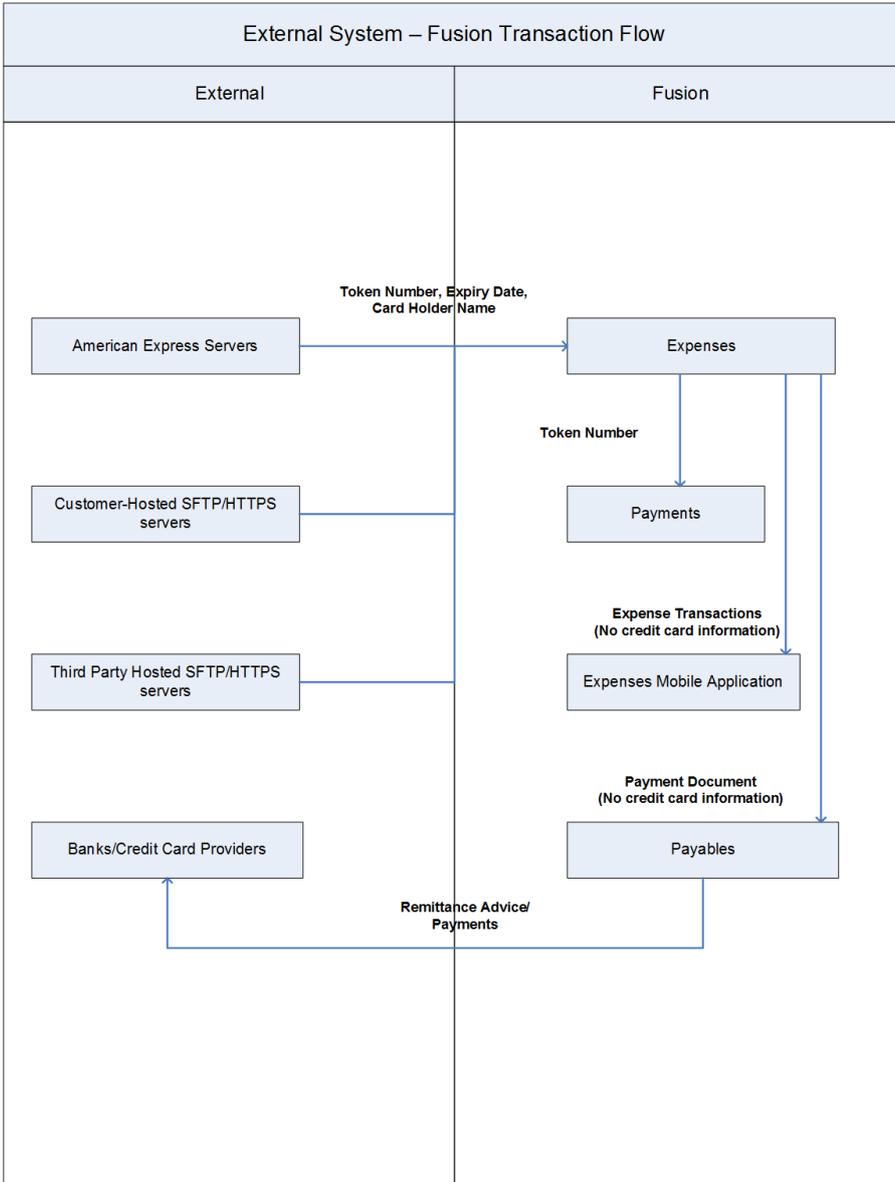
Oracle Fusion Payments Card Tokens Import with Transactions

- Oracle Fusion Payments provides capability to interface legacy credit card data into Oracle ERP Cloud.
- In this flow, the credit card number, card holder name, card brand, expiry date, billing address, and email address are first interfaced into CyberSource wherein the card number is tokenized and is returned along with other card holder data in an output file.
- The tokenized card number, expiry date, card holder name, card brand, and billing address are then interfaced into Oracle Fusion Payments using web service.



Corporate Card File Import Flow - Expenses

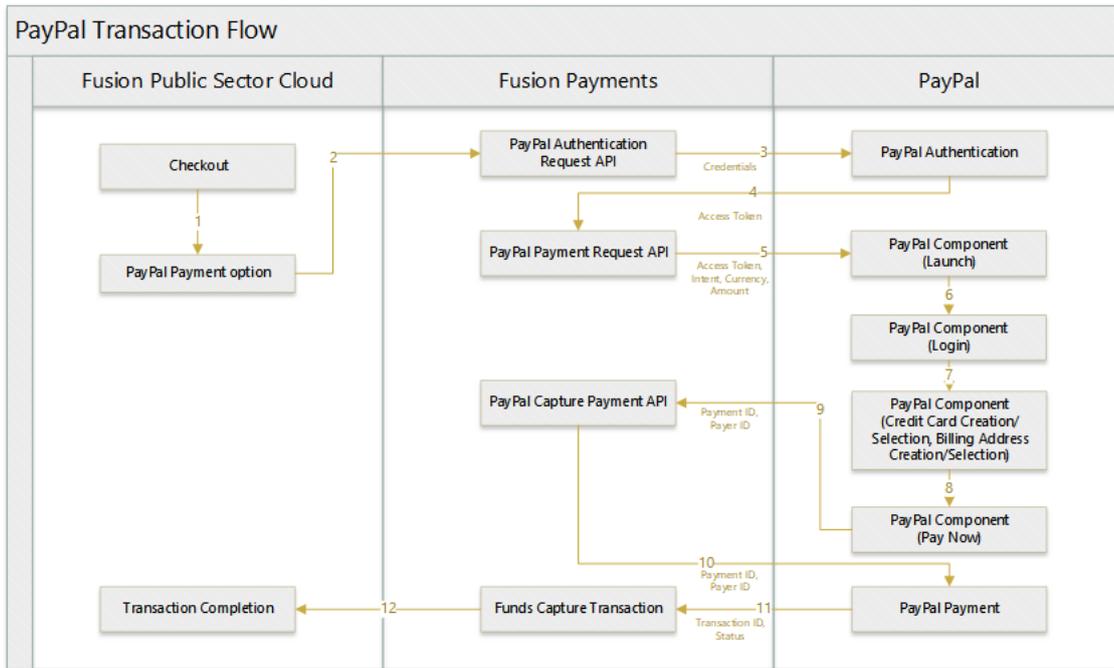
- Oracle Fusion Expenses can receive and process tokenized card numbers for American Express and Visa and truncated card numbers for Mastercard.
- Corporate card administrators can only view tokenized card numbers in Oracle Fusion Expenses.
- The tokenized card numbers are stored in Oracle Fusion Payments.



Pay via PayPal flows

1. As part of the cart checkout flow, user comes to the calling application's payment page which has the Oracle Fusion Payments shared UI component embedded. When the user selects the PayPal option, the Payments UI component shows the PayPal Smart Payment button embedded.
2. Clicking the PayPal Smart Payment button opens the PayPal page in a dialog box. User enters the credentials to sign in.
3. User either selects an existing credit card and billing address or creates a new one. User then clicks Pay Now which makes the payment with PayPal.
4. Once payment is completed, a confirmation message is shown on the calling application's UI.

High-level flow diagram



Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2022, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.