CHAPTER 1

Setting Up ePayment Processing

This chapter includes an overview of ePayment processing and discusses how to:

- Set up credit card types.
- Re-encrypt credit card, bank account numbers, Security Code data, and Security Key.
- Set up Payment merchants.
- Test Payment and Hosted Payment Transactions.
- Set up Student Financials merchants.
- Set up institution sets.
- Set up item types for an ePayment transaction.
- Set up self-service payment messages.
- Set up self-service options.

Understanding ePayment Processing

Feature Pack 2

A new flexible Application Class-based interface has been created to support the processing of credit card and eCheck transactions. This ePayment API application class supports both Integration Broker and Business Interlink technology. Included in Feature Pack 2 is support for Integration Broker and Hosted Payment processing and support for the credit card Security Code. Finally, there is a change to Admissions Application Fee Payment.

Hosted Payment: The new Hosted Payment feature allows you to use a third party payment provider to collect and store credit card and bank account information. Any web services required to authorize or credit the transaction will be routed through the new ePayment API.

Support for Security Code: The Security Code that is located on credit cards is a security feature for “card not present” transactions such as Internet transactions. You can lower your per transaction costs and increase fraud deterrence if you collect the Security Code as part of the credit card transaction. The Security Code is supported only if you use the new Integration Broker interface and not Business Interlink.

Admissions: You can no longer authorize/capture credit card payments through Admissions Application Fee Payment.

For documentation about these features, refer to updates in this chapter, and to the other chapters and the Developer Guide in the Feature Pack documentation.
Student Financials enables your institution to receive payments for charges by eCheck or credit card through cashiering (credit card only) and over the web using self-service functionality (credit card and eCheck). The rules that your institution defines for authorizing and capturing ePayment transactions as well as for processing ePayment credits are established when you set up your payment merchant, SF merchant, and SF institution set parameters.

Setting Up Credit Card Types

To set up credit card types, use the Credit Card Type component (CREDIT_CARD_TYPE).

Your institution must have contracts with credit card providers (such as VISA or Master Card) to be able to accept payments using their cards. To prevent users from attempting to record payments using unauthorized cards, you must define the credit card types accepted by your institution.

This section discusses how to define accepted credit card types.

**Page Used to Set Up Credit Card Types**

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Type</td>
<td>CREDIT_CARD_TYPE</td>
<td>Set Up SACR, Product Related, Student Financials, Credit Card Type</td>
<td>Define accepted credit card types.</td>
</tr>
</tbody>
</table>

Defining Accepted Credit Card Types

Access the Credit Card Type page (Set Up SACR, Product Related, Student Financials, Credit Card Type).

**Credit Card Type**

SetID: FSUNY  Credit Card Type: VI

Description: Visa Card

Short Description: Visa Card

**Date Format**

- **MM/DD/YYYY**
- **MM/YYYY**

Credit Card Type page

**Date Format**

Select an expiration date format.

**MM/DD/YYYY** Select to include the month, day, and year in the expiration date format.
Re-encrypting Credit Card, Bank Account Numbers, Security Code Data, and Security Key

Feature Pack 2: Security Code

Security Code data is stored encrypted in a new table (SSF_PAYMENT_CVV) until it is authorized. The row is deleted immediately after authorization.

The Security Code shares the same Encryption Profile as credit card and account numbers.

For more information about support for the Security Code, refer to the Setting up Payment Merchants and Setting Up SF Merchants sections later in this chapter.

For more information about encryption of Security Code data, refer to the Completing Student Financials General Setup chapter.

For information about the storage of the Security Code, including the new purge process, refer to the Processing ePayment Transactions chapter.

Security Code and CVV (Card Verification Value) are used interchangeably in the documentation.

To replace a known or suspected compromised encryption key, regenerate the encryption key and convert existing credit card, bank account numbers, and Security Code data using the new key. Periodic key changes can be essential to your institution’s encryption key management.

This section provides overviews of encryption and re-encryption and discusses how to:

- Regenerate the encryption key.
- Convert data to use a regenerated encryption key.

Understanding Encryption

PeopleSoft Enterprise Campus Solutions encryption uses PeopleTools Pluggable Cryptography, which is an advanced security framework that provides a security model for applications to encrypt credit card data.

Pluggable Cryptography enables you to secure critical PeopleSoft data and communicate securely with other businesses. It enables you to extend and improve cryptographic support for your data in PeopleTools, giving you strong cryptography with the flexibility to change and grow, by incrementally acquiring stronger and more diverse algorithms for encrypting data. In PeopleTools, pluggable cryptography capability is provided by PeopleSoft pluggable encryption technology (PET).

By using the Tools Pluggable Cryptography for strong encryption/decryption, the system encrypts data using 3DES algorithms and 168-bit encryption keys.

To replace a known or suspected compromised key, regenerate the encryption key and convert existing credit card, bank account numbers, and Security Code data using the new key. Periodic key changes can be essential to your institution’s encryption key management.

This section provides an overview of how to regenerate the encryption key and convert credit card, bank account numbers, and Security Code data using the new key.
**Understanding Re-encryption**

When you change the encryption key at any time after the initial conversion, you must also re-encrypt all of your credit card, bank account numbers, and Security Code data using that key. Predefined encrypt and decrypt profiles are delivered for Campus Solutions re-encryption. These profiles specify multiple user-defined steps applying various algorithms and keys to the data in a specified order and supporting various encryption standards and third-party encryption libraries.

Use the following parameters for Campus Solutions re-encryption.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Profile ID</td>
<td>CS_CREDIT_CARD_ENCRYPT</td>
</tr>
<tr>
<td>Algorithm ID (encrypt)</td>
<td>3des ks168 cbc_encrypt</td>
</tr>
<tr>
<td>Keyset ID</td>
<td>CSCreditCard</td>
</tr>
<tr>
<td>Decrypt Profile ID</td>
<td>CS_CREDIT_CARD_DECRYPT</td>
</tr>
<tr>
<td>Algorithm ID (decrypt)</td>
<td>3des ks168 cbc_decrypt</td>
</tr>
</tbody>
</table>

**Note.** You can create your own profiles or modify the delivered ones. However, we do not recommend it. If you do, you must be very careful to use the appropriate values for whatever you create or modify.

To change the credit card encryption key and re-encrypt the data, do the following:

1. Navigate to the Generate Encryption Key page (Set Up SACR, Common Definitions, Encryption, Generate Encryption Key).
2. Click the Generate Random Key button to generate a new random hexadecimal encryption key. Clicking this button generates a new, random hexadecimal encryption key. You can modify this key. However, you must format it as a 24-byte string in hexadecimal notation. The first two characters must be 0x, and the remainder must be exactly 48 characters consisting of a combination of numeric digits and the lowercase letters a through f.
3. Copy the regenerated encryption key.
4. Navigate to the Algorithm page (PeopleTools, Security, Encryption, Algorithm Keyset) for the encrypt algorithm ID and keyset ID (3des ks168 cbc_encrypt and CSCreditCard).
5. Paste the regenerated encryption key value in the Key Value field, replacing the previous value, and save the page.
7. Confirm that the encrypt and decrypt profile IDs are correct, then click the Run button to start the conversion process.
   The Credit Card Conversion process converts each field in the grid. If the process fails for any reason, the process can be restarted in the standard way and the process picks up where it left off. If the process cannot be restarted, the process can be run from the beginning and it automatically bypasses fields that have already been processed.

**Warning!** You must complete steps 1-7 to encrypt and run the conversion process prior to completing the next steps, which set up decryption.

8. Navigate back to the Algorithm page (PeopleTools, Security, Encryption, Algorithm Keyset) for the decrypt algorithm ID and keyset ID (3des ks168 cbc_decrypt and CSCreditCard).
9. Paste the regenerated encryption key value in the Key Value field, replacing the previous value, and save the page.

See Also

PeopleSoft Enterprise PeopleTools PeopleBook: Security Administration, “Securing Data with Pluggable Cryptography”

PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Completing Student Financials General Setup, Defining Keyword Edit Tables and a Null Due Date

PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Processing ePayment Transactions

## Pages Used to Re-Encrypt and Convert Data

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate Encryption Key</td>
<td>SSF_CC_ENCRYPT_KEY</td>
<td>Set Up SACR, Common Definitions, Encryption, Generate Encryption Key</td>
<td>Use this utility to change the key used to encrypt credit card, bank account numbers, Security Code data, and Security Key. <strong>Note.</strong> When you change the key, you must also run the conversion utility to re-encrypt credit card numbers using the new encryption key. Never change the key without also running the conversion.</td>
</tr>
<tr>
<td>Convert Encryption</td>
<td>SSF_CC_RUN_CNVRT</td>
<td>Set Up SACR, Common Definitions, Encryption, Convert Encryption</td>
<td>Perform conversion of credit card numbers to use a regenerated credit card encryption key.</td>
</tr>
<tr>
<td>Algorithm Keyset</td>
<td>CRYPT_KEYSET</td>
<td>PeopleTools, Security, Encryption, Algorithm Keyset</td>
<td>Copy the regenerated key to the key value field on this page for the encrypt profile prior to running the conversion process. After running the conversion process, copy the regenerated key to the key value field on this page for the decrypt profile.</td>
</tr>
<tr>
<td>Process Scheduler</td>
<td>PRCSRQSTDLG</td>
<td>Click the Run button on the Convert Encryption page.</td>
<td>Run the SSF_CC_CNVRT conversion process to convert existing credit card data using the regenerated credit card encryption key.</td>
</tr>
</tbody>
</table>

## Regenerating the Encryption Key

Access the Generate Encryption Key page (Set Up SACR, Common Definitions, Encryption, Generate Encryption Key).
Generate Encryption Key

Generate Random Key

Click to have the system generate a random key in the format needed by the encryption algorithms used for credit card encryption and decryption profiles.

Converting Data to Use a Regenerated Encryption Key

Access the Convert Encryption page (Set Up SACR, Common Definitions, Encryption, Convert Encryption).
Chapter 1 Setting Up ePayment Processing

**Convert Encryption**

**Run Control ID:** PS

**Decryption Profile ID**  
**Encryption Profile ID**

<table>
<thead>
<tr>
<th>Record (Table) Name</th>
<th>Field Name</th>
<th>Crypt Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM_APPL_TENDER</td>
<td>CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>ADM_APPL_TENDER</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_EP_ADJ_GIFT</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_EP_ADJ_MBR</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_EP_GIFT_DTL</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_EP_MER_DTL</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_EP_TRNS_LOG</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>AV_INVLV_O_HDR</td>
<td>AV_CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>CSH_OFF_RCPT_T</td>
<td>CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>CSH_OFF_RCPT_T</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>GROUP_LINE</td>
<td>CREDIT_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>GROUP_LINE</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>PAYMENT_TBL</td>
<td>CREDIT_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>PAYMENT_TBL</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>QUICK_POST_TBL</td>
<td>CREDIT_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>QUICK_POST_TBL</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>REFUND_CC_INFO</td>
<td>CREDIT_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>REFUND_CHECK</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>SF_ACCT_PROFILE</td>
<td>CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>SF_ACCT_PROFILE</td>
<td>SSF_BNK_ACCT_NUM</td>
<td>Decrypt, then Encrypt</td>
</tr>
<tr>
<td>SF_PAYMENT</td>
<td>CR_CARD_NBR</td>
<td>Decrypt, then Encrypt</td>
</tr>
</tbody>
</table>

Convert Encryption page

**Decryption Profile ID** and **Encryption Profile ID**

Default profile IDs are set on the SF Installation 2 page (Set Up SACR, Install, Student Fin Installation, SF Installation 2).

PeopleTools Pluggable Cryptography framework provides the delivered profiles of *TRIPLE DES ENC B64* and *TRIPLE DES DEC B64*.

PeopleSoft Enterprise Campus Solutions has enhanced the PeopleTools profiles specifically for Campus Solutions reencryption. The predefined, enhanced profiles delivered for Campus Solution are *CS_CREDIT_CARD_DECRYPT* and *CS_CREDIT_CARD_ENCRYPT*.

Profiles specify multiple user-defined steps applying various algorithms and keys to the data in a specified order and supporting various encryption standards and third-party encryption libraries.

The decrypt profile must be the same profile and have the same keys used to encrypt the data as it is. The encryption profile must contain the new
Setting Up Payment Merchants

Feature Pack 2

A new flexible interface has been created to support the processing of credit card and eCheck transactions. This new interface uses a flexible adapter-based model to support the transmission of electronic payment transactions. You can choose to use the existing Business Interlinks or a new Integration Broker-based interface to send electronic payment transactions to third party payment processors.

Before you read the following section in this chapter, refer to the new Setting Up Adapters chapter in the Feature Pack documentation for information about the new Adapter Type Table and Adapter Table components that are used to define the adapters used by the electronic payment API. (The new chapter will be located in the Application Fundamentals PeopleBook.)

This section discusses the new Payment Merchant component and the new Electronic Payment Test component.

A flexible interface supports the processing of credit card and eCheck transactions. The interface uses a flexible adapter-based model to support the transmission of electronic payment transactions. You can use either the Integration Broker-based interface or the Business Interlinks interface to send electronic payment transactions to third party payment processors. The Integration Broker interface provides Security Code support but the Business Interlinks interface does not.

Warning! Before you read this section, refer to the Setting Up Adapters chapter in the Application Fundamentals PeopleBook for information about the Adapter Type Table and Adapter Table components. The components are used to define the adapters that are used in electronic payment and hosted payment processing.

See: PeopleSoft Enterprise 9.0 Application Fundamentals PeopleBook, Setting Up Adapters

Feature Pack 2

The new Payment Merchant component is used to define electronic payment merchants and support the new ePayment API.

The Payment Merchant is used to define interface–related merchant settings. The SF Merchant is still used and now has a pointer to the new Payment Merchant component.

To set up Payment merchants, use the Payment Merchant (SCC_MERCHANT) component.

This section discusses how to define Payment merchants.
Page Used to Set Up Payment Merchants

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Merchant</td>
<td>SCC_MERCHANT</td>
<td>Set Up SACR, Common Definitions, Electronic</td>
<td>Define electronic payment merchants.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Payments, Payment Merchant, Payment Merchant</td>
<td></td>
</tr>
</tbody>
</table>

Defining Electronic Payment Merchants

Access the Payment Merchant page (Set Up SACR, Common Definitions, Electronic Payments, Payment Merchant, Payment Merchant).

Feature Pack 2:
The following fields have been removed from the SF Merchants page and added to this new Payment Merchant page: Service Provider, Process Server, IP Override, Verification Level, and Settlement Method.
The Address Verification Flag field appears on both the SF Merchants page and this new Payment Merchant page.

Payment Merchant

Merchant Setup ID: HostedPaySiteCC

*Description: Hosted Site for Credit Card

*Status: Active

*Service Provider: TouchNet

*3rd Party Merchant ID: 47

Hosted Payment Setup

Adapter: SCC_MODE1A

Browser Requirements Message:
To proceed with your payment, you need to enable cookies and Javascript in your browser. If you are unsure how to enable these, please click on the Browser Requirements link below.

Browser Requirements Detail:

How to Enable Cookies:
Microsoft Internet Explorer 6 or later Choose Tools -- Internet Options. Click the Privacy tab
Service Provider

**Feature Pack 2 Moved from SF Merchants page**

Select a service provider: Cybersource, TouchNet, or Unsupported. This field is informational only.

3rd party Merchant ID

Enter the merchant name.

Hosted Payment Provider

Select this check box to identify the payment merchant as a hosted payment provider.

If you select this check box:

- The Hosted Payment Setup group box becomes available.
- The CVV Supported check box in the Credit Card group box is not available, because that control is established (as well as collected) at the hosted payment (third party) site.

See: PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Processing ePayment Transactions
Chapter 1 Setting Up ePayment Processing

Hosted Payment Setup

This group box is available only if the Hosted Payment Provider check box is selected.

**Adapter**
Select the adapter to be used by the hosted payment merchant to process hosted payment transactions.

**Browser Requirements Message and Browser Requirements Detail**
Enter a browser-related message, or browser-related detail about browser requirements, that an application can display to a user before the user is transferred to the third party hosted site.

**Browser Requirements Message**
For schools that use hosted payment, the message that you enter here appears on the Make a Payment - Confirm Payment page if the Display Browser Message check box is selected on the Electronic Payments (Institution Set) setup page.

**Browser Requirements Detail**
For schools that use hosted payment, the detail that you provide here appears when students click the Browser Requirements link on the Make a Payment - Confirm Payment page if the Display Browser Message check box is selected on the Electronic Payments (Institution Set) setup page.

See PeopleSoft Enterprise Campus Self Service 9.0 PeopleBook, Setting Up Student Financials Self Service, Defining Self-Service Electronic Payments for Institution Sets

Electronic Payment Setup

**Service Operation**
Select the service operation to be used by the adapter when processing the electronic or hosted payment transaction request. This field is required only if you use the Integration Broker based adapter (SCC_INT_BROKER).

**Adapter**
Select the adapter to be used by this merchant to process electronic payment transactions using the electronic payment interface.

**Insert All Transactions**
Click this button to insert all transactions into the Supported Transactions group box.

**Security Key Required**
Use this check box to indicate that a special security token or password is needed to process transactions. If you select this check box, the Security Key Setup group box becomes available.

Security Key Setup

This group box is available only if you select the Security Key Required check box.

**Key**
This field contains the security token or password that might be required by a third party payment processor. This field is encrypted using the encryption profiles from the SF Installation table.

Supported Transactions

The following services are available for the ePayment API. Check with your third party provider for a list of supported services.

**Value**
Select a value for the supported transactions.

Credit Card transactions:
Setting Up ePayment Processing

Chapter 1

- 1: Authorize Only
- 2: Authorize and Bill
- 3: Bill Only
- 4: Credit Only

eCheck transactions:
- 5: Make Payment
- 6: Apply Credit

Hosted transactions:
- 91: Get Token
- 92: Authorize Only
- 93: Credit Only

Electronic Check

Verification Level

**Feature Pack 2**
Moved from the SF Merchants page

Select the level of verification that the system uses for eCheck payments. If a valid value is not entered on the transaction request, the value that you select here is used.

*Validation:* Select to test the format and bank routing number of each eCheck payment and to compare the transaction information to the check-processing partner’s internal negative file.

*Verification:* Select to perform all validation steps and to compare each transaction’s information with an external negative file to identify accounts that have a history of bad checks or that were closed for cause.

**Note.** Validation and verification are optional. Neither process checks the status or the existence of an account nor do they guarantee that funds are available.

Settlement Method

**Feature Pack 2**
Moved from the SF Merchants page

Select the default method that the system uses to deliver settlements to and from your students’ banks.

If a valid value is not entered on the transaction request, the value that you select here is used.

*Automated Clearing House:* Select to deposit U.S. and Canadian transactions using the Automated Clearing House (ACH) or the Canadian Payment Association.

*Facsimile draft:* Select to deposit transactions as facsimile drafts. Use this method when the issuing bank is not an ACH member.
**ACH Class**

Select the default value for ACH Class data element used by eCheck transactions. If a valid value is not entered on the transaction request, the value that you select here is used.

The values are:

1. **ARC** (Accounts Receivable Entries): Checks received by a merchant through mail or drop box and presented as a HYPERLINK "http://www.nationalach.com" ACH entry.
2. **POP** (Point-of-Purchase): A check presented in-person to a merchant for purchase is presented as a HYPERLINK "http://www.nationalach.com" ACH entry instead of a physical check.
3. **TEL** (Telephone Initiated-Entry) Verbal authorization by telephone to issue a HYPERLINK "http://www.nationalach.com" ACH entry such as checks by phone.
4. **WEB** (Web Initiated-Entry): Electronic authorization through the Internet to create a HYPERLINK "http://www.nationalach.com" ACH.

**Credit Card**

**CVV Supported**

Select this check box to indicate that the merchant supports the sending of Security Code values.

You must clear this check box for merchants using Business Interlink based integration technology.

Because the Security Code is captured at the third party site for hosted payment transactions, this check box is not available for hosted payment providers—that is, where the Hosted Payment Provider check box is selected.

See PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Processing ePayment Transactions

**Address Verification Flag**

This field controls whether the system verifies the credit card billing address during credit card processing. The options are Address Verification Off and Address Verification On.

**Note.** If you select Address Verification On and the address given does not match, authorization is declined, but the credit card funds are set aside.

If a valid value is not entered on the transaction request, the value that you select here is used for credit card transactions.

This field also appears on the SF Merchants page.

**Additional Setup Options**

**Process Server**

**Feature Pack 2**

Moved from the SF Merchants page
This field holds the location of the Process Server used by the Business Interlink based credit card and eCheck transactions. This field is only relevant if you are using the Business Interlinks and the Business Interlink adapter (SCC_BUS_INTERLINK).

**IP Override**

**Feature Pack 2**

Moved from SF Merchants page

This field is used by the credit card and eCheck business interlinks and is passed through the ip_address input property. This field is also used as a default ip address for transactions processed by the Integration Broker based adapter for electronic payment transactions that require this field.

See Electronic Payment Integration Developer’s Reference Guide. The guide is posted to My Oracle Support.

**See Also**

*PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Processing ePayment Transactions*

## Testing Payment and Hosted Payment Transactions

**Feature Pack 2**

New component: Electronic Payment Test component allows testing of the various ePayment and hosted payment transactions. This page also serves as a run control page for the batch testing component (SCC_EPAY_TST – Epayment Batch Test). The existing RUNCTL_SFPCRTEST Business Interlink Test component and page remains.

Refer to the following documentation for more information.

The Electronic Payment Test component allows testing of ePayment and hosted payment transactions. This page also serves as a run control page for the batch testing component (SCC_EPAY_TST – Epayment Batch Test).

**Page Used to Test Payment and Hosted Payment Transactions**

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Payment Test</td>
<td>SCC_EPAYMENT_TEST</td>
<td>Set Up SACR, Common Definitions, Electronic Payments, Electronic Payment Test</td>
<td>Test epayment and hosted payment transactions.</td>
</tr>
</tbody>
</table>

**Testing ePayment and Hosted Payment Transactions**

Access the Electronic Payment Test page (Set Up SACR, Common Definitions, Electronic Payments, Electronic Payment Test).
Chapter 1

Electronic Payment Test

Run Control ID: BILLING

Merchant Options
- Merchant Setup ID: HostedPaySiteCC
- 3rd Party Merchant ID: 35
- Adapter ID: SCC_INT_BROKER
- Adapter Class: SCC_EPAYMENT_ADAPTERS\IntegrationBroker\Adapter
- Service Operation: SCC_UPAY_SYNC
- ACH Class: POP

Testing Options
- Trans. Type: [ ]
- Payment Amount: 100.00 USD
- Merchant RefId: e1ee2f24-6f08-11e1-b841-b36d2053e00

Transaction Response
- Result Code: 0
- Original Result Code: 100
- Decision: SUCCESS
- Status Message: Transaction was successful.
- AVS Code: X
- CV Result: M
- Transaction Ref: 613738377WATK5J0
- Request ID: 2459801789370098401927

Electronic Payment Test page (1 of 3)
### Post to Hosted Payment URL
Click this button to cause a redirect to the third party URL where a sample payment can be made. The third party site should redirect you back to this page after the payment is made. You can then authorize the payment by using the Trans. Type field to select the Authorize Only (92) transaction.

**Note.** The Session ID field should be updated after you select either Authorize Only (92) or Credit Only (93) transaction.

This button is available only for payment merchants who are hosted payment providers.

### Submit
Click this button to submit the transaction using the Electronic Payment API.

### Run
Click this button to run the batch electronic payment test program. This program tests credit card and eCheck transactions (Authorize and Credit) to make sure that these transactions function correctly in a batch environment (this is more relevant when using the Business Interlink adapter).

### Merchant Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Setup ID</td>
<td>Select a Merchant Setup ID. Values are defined in the Payment Merchant setup component (Set Up SACR, Common Definitions, Electronic Payments, Payment Merchant, Payment Merchant).</td>
</tr>
</tbody>
</table>

**Note.** The remaining fields in this section are informational only and appear based on the setup in the Payment Merchant setup component and the Adapter Type Table and Adapter Table setup components.

### Testing Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trans. Type (transaction type)</td>
<td>Select the type of transaction to be processed. The valid values for this field are defined in the Supported Transactions section of the Payment Merchant setup page (Set Up SACR, Common Definitions, Electronic Payments, Payment Merchant, Payment Merchant).</td>
</tr>
<tr>
<td>Merchant Ref ID</td>
<td>Enter a value that uniquely identifies the transaction that is sent to the third party processor. If this field is left blank it is programmatically populated with a uniquely generated ID.</td>
</tr>
</tbody>
</table>

### Transaction Response
This section of the page contains the results of the transaction request. The fields all appear based on properties of the Transaction Response class that is returned from the Electronic Payment Manager class.

### See Also
*PeopleSoft Enterprise Student Financials 9.0 PeopleBook*, Setting Up ePayment Processing, Setting Up ePayment Merchants

## Setting Up SF Merchants
To set up SF merchants, use the SF Merchants (MERCHANT_TBL) component.
This section provides an overview of SF merchants and discusses how to define ePayment processing parameters.

**Understanding SF Merchants**

**Feature Pack 2**

*You can no longer authorize/capture credit card payments through Admissions Application Fee Payment. The SF Merchant ID field has been removed from the Application Center Table page.*

An SF merchant (student financials merchant) is an entity within the Student Financials application that enables you to set up unique credit card and eCheck processing rules for different departments in your institution. You can use an SF merchant to set up credit card and eCheck processing for cashiering offices and student self-service functions. The SF merchant definition provides information needed by the ePayment service provider and defines what services it performs and what customer information the system displays on the payment page.

To process credit cards and eChecks in Student Financials, you must establish at least two SF merchant definitions—one for credit card support and one for eCheck support. If you have different processing rules for credit card processing in the cashiering office than you do in student self service, then you will need to establish multiple credit card SF merchants to handle these different processing rules.

**Page Used to Set Up SF Merchants**

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF Merchants</td>
<td>MERCHANT_TBL</td>
<td>Set Up SACR, Common Definitions, Self Service, Student Financials, SF Merchants</td>
<td>Define ePayment processing parameters. Used for cashiering offices and student self service.</td>
</tr>
</tbody>
</table>

**Defining ePayment Processing Parameters**

Access the SF Merchants page (Set Up SACR, Common Definitions, Self Service, Student Financials, SF Merchants).
## SF Merchants

<table>
<thead>
<tr>
<th>SF Merchant ID:</th>
<th>ECHKCRCARD</th>
</tr>
</thead>
<tbody>
<tr>
<td>'Description:'</td>
<td>eCheck Credit Card Merchant</td>
</tr>
<tr>
<td>'Process Option:'</td>
<td>Credit Card</td>
</tr>
<tr>
<td>'Payment Merchant:'</td>
<td>CyberSource Int Broker 1</td>
</tr>
<tr>
<td></td>
<td>□ Hosted Payment Provider</td>
</tr>
<tr>
<td></td>
<td>✓ CVV Supported</td>
</tr>
</tbody>
</table>

**Batch Transmission Error:**

<table>
<thead>
<tr>
<th>Credit Card</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Real-Time Authorization</td>
<td>✓ Real-Time Capture</td>
</tr>
<tr>
<td>✓ Real-Time Credit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perform Check Risk Service</th>
<th>Check Risk Threshold:</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Check Digit Edit</td>
<td></td>
</tr>
<tr>
<td>☑ CVV Required</td>
<td></td>
</tr>
<tr>
<td>'Address Verification Flag':</td>
<td>Address Verification Off</td>
</tr>
</tbody>
</table>

### Self Service Options

| Convenience Fee Option:     |                          |
|                            |                          |
| Convenience Fee Amount:     |                          |
| Convenience Fee Percentage: |                          |
| Minimum Payment Amount:     | 10 000                   |
| Maximum Payment Amount:     | 1000 000                 |

### Default Options

<table>
<thead>
<tr>
<th>Contact Type:</th>
<th>☑</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Usage:</td>
<td>BILLING</td>
</tr>
<tr>
<td>Type of Name:</td>
<td>Primary</td>
</tr>
<tr>
<td>Phone Type:</td>
<td>Main</td>
</tr>
<tr>
<td>Email ID:</td>
<td>☑ Default Email</td>
</tr>
</tbody>
</table>

| ps@ps.com       |                          |
**Feature Pack 2:**

Changes to the SF Merchants page:
The following fields have been removed from this page and added to the new Payment Merchant setup page: Service Provider, Process Server, IP Override, Verification Level, and Settlement Method.
The following fields have been added to this page: Hosted Payment Provider, CVV Supported, and CVV Required.
The Address Verification Flag field appears on both this page and the new Payment Merchant page.
The Merchant ID field is replaced with the Payment Merchant field. Values available in the Payment Merchant field are based on the values that you define in the Merchant Setup ID field on the new Payment Merchant page.
The Real-Time Settlement check box is now the Real-Time Capture check box.

**Process Option**
Select the type of transaction that is governed by the SF Merchant rules that you are defining: **Credit Card** or **Electronic Check**.

**Payment Merchant**
Enter the Payment Merchant that you wish to use for this SF Merchant. The ID can be shared by several SF Merchant definitions.

---

**Note.** If you intend to process both credit card and eCheck self-service transactions, you must set up two SF merchants, one with a process option of **Credit Card** and one with a process option of **Electronic Check**.

**Hosted Payment Provider**
**Feature Pack 2**
**New field**
If the payment merchant that you select on this page is a hosted payment provider and you selected the Hosted Payment Provider check box on the Payment Merchant page, the check box on this page appears selected and unavailable for edit.

If the payment merchant that you select on this page is not a hosted payment merchant, the Hosted Payment Provider check box appears on this page but is cleared and is not available for edit.

**CVV Supported**
**Feature Pack 2**
**New field**
If you selected the CVV Supported check box on the Payment Merchant page to indicate that the merchant supports the sending of Security Code values, the check box on this page appears selected and unavailable for edit.

This check box does not appear for hosted payment providers.

**Batch Transmission Error**
Enter the maximum number of batch transmission errors that you want the system to allow before canceling the batch transmission.

**Credit Card**
This group box appears if you select **Credit Card** in the Process Option field. Use it to enter credit card–specific processing parameters. Check with your third party provider for a list of supported services.

**Real-Time Authorization**
Select to authorize credit card transactions in real time, actually reserving or setting aside credit card funds. If you clear this check box, you must authorize credit card transactions in batch mode. When you select this check box, the Real-Time Capture check box becomes available.
Chapter 1 Setting Up ePayment Processing

Real-Time Capture
Select to capture credit card transactions in real time, actually transferring funds to your institution as the transaction takes place. If you clear this check box, you must capture credit card transactions in batch mode.

For hosted payment providers, this check box is selected and is not available for edit.

Real-Time Credit
Select to credit in real time when you void credit card payments originating from cashiering offices.

Note. Do not select this check box for self-service transactions because you can only process credits for self-service transactions in batch.

Perform Check Risk Service
Select to perform a risk assessment at the time of authorization. The risk assessment is an estimation of the veracity of the transaction. Factors such as improper address, too many transactions, or transactions dispersed geographically increase the risk of fraud.

This check box is not available for hosted payment providers.

Check Digit Edit
Select to verify the check digit of the credit card number being used prior to processing the transaction. If the check digit is incorrect, the customer receives an error message and is asked to correct the credit card number entered.

This check box is not available for hosted payment providers.

Check Risk Threshold
Enter an amount above which the credit card processing merchant is alerted to the possibility of fraud. When a transaction is processed, the credit card processing vendor returns a risk assessment. The check risk threshold is the allowable risk that a school is willing to assume for a given transaction.

This check box is not available for hosted payment providers.

CVV Required (Card Verification Value required)

Feature Pack 2

New field

The Security Code is supported only if you use the new Integration Broker interface for credit card processing.

This check box is available only for credit card merchants.

The check box does not appear if the merchant is a hosted payment provider.

If you select this check box, the Security Code field or CVV field is available as a required field on all pages that accept credit card transactions—Cashiering, Make a Payment, and Purchase Miscellaneous Items.

The Security Code or CVV field does not appear on any inquiry pages.

Note. The Security Code is supported only if you use the Integration Broker interface for credit card processing. Do not select the check box if you use Business Interlinks.

Address Verification Flag
This field controls whether the system verifies the credit card billing address during credit card processing. The options are Address Verification Off and Address Verification On.
**Note.** If you select *Address Verification On* and the address given does not match, authorization will be declined, but the credit card funds will be set aside.

This field appears on this page and the Payment Merchant page.

### Electronic Check

This group box appears if you select *Electronic Check* in the Process Option field. Use it to enter eCheck-specific processing parameters. Check with your third party provider for a list of supported services.

#### Real-Time Debit

Select to process eCheck transactions in real time. If you clear this check box, you must run the eCheck Processing process to debit eCheck payments in batch.

#### Authentication Method or Shared Secret

For Integration Broker and Business Interlinks, the field appears as Authentication Method.

Define how the system authenticates eCheck payments. If you select *Birthdate, PIN, or National ID Number*, students must enter the required information to authenticate an eCheck payment. If you select *No Authentication*, students can submit eCheck payments without authentication.

You define a student’s birthdate, national ID number, or PIN in PeopleSoft Campus Community. The system always uses a student’s primary national ID number for authentication purposes.

For Hosted Payment, the field appears as Shared Secret.

When the third party payment provider authenticates the student on their site, they use the Shared Secret provided by Campus Solutions to verify the student. Valid values are *PIN* and *Birthdate*.

**Note.** Students should not use dashes when entering the national ID number.

See Iscc, Managing Personal Identification Data, Entering PINs.

See Iscc, Adding a Person to Your Campus Solutions Database.

See Iscc, Managing Biographical Information.

### Self Service Options

#### Convenience Fee Option

Select one of the following options if you want to charge students a fee for each ePayment transaction.

*Fixed Amount:* Select to charge a fixed convenience fee for each ePayment transaction.

*Percentage:* Select to make the convenience fee equal a percentage of the ePayment transaction.
Note. In most cases, the ePayment convenience fee is posted wherever the payment is applied. For example, if a payment is allocated to charges across multiple business units, the convenience fee is based on the total payment, but is distributed proportionately across the business units. If the payment is not allocated across business units but is directed to charges in one business unit, the convenience fee will be posted in the same business unit. If a payment is not manually allocated, the convenience fee is directed to the business unit with the highest priority.

Convenience Fee Amount
If you want to charge a fixed convenience fee amount, specify the amount as currency. (For example, using U.S. Dollars as the base currency, an entry of 1.50 results in a surcharge of 1.50 USD per transaction).

Convenience Fee Percentage
If you want to charge a percentage convenience fee, specify the percentage as a number greater than zero. In the previous example, the entry 5.5 results in a surcharge of 5.5 percent per transaction.

Minimum Payment Amount
Set the minimum amount that a student can pay during a single ePayment transaction.

Maximum Payment Amount
Set the maximum amount that a student can pay during a single ePayment transaction.

Default Options
Items in this group box relate to customer information that the system displays on the Make a Payment page for self-service transactions, and the Tender Details page for cashiering transactions.

Contact Type
Select the contact type representing the address for an External Org ID.

Address Usage
Select the address usage type that you want to use to display default customer addresses on the payment page.

Default Email
ePayment processing vendors require an email address to process transactions. Select this check box to use the default email address entered in the Email ID field rather than requiring students to enter one. When you select this check box, the Email Address field does not appear on the Make a Payment self-service page.

Type of Name
Select the default name type that the system uses to look up and display the customer name on the Make a Payment page.

Phone Type
ePayment processing vendors require a phone number to process transactions over the web. Select the default phone type that the system uses to look up and display the customer phone number on the Make a Payment page.

Email ID
Enter the default generic email address that the system uses for all credit card transactions when you select the Default Email check box.

See Electronic Payment Integration Developer’s Reference Guide. The guide is posted to My Oracle Support.

See Also
PeopleSoft Enterprise Student Financials 9.0 PeopleBook, Processing ePayment Transactions
Setting Up Institution Sets

You use institution sets to define basic institution set parameters and to set up ePayment rules for institution sets. This setup is done in Campus Self Service.

See Isss, Setting Up Student Financials Self Service, Setting Up Institution Sets.

Setting Up Item Types for ePayment

To enable eCheck and credit card processing, you must define miscellaneous parameters for item types. The system uses the following attributes from the credit card or eCheck Item Type, Miscellaneous page:

- Charge Priority List (during posting of the ePayment transaction).
- Payment Overall Priority (during posting of the ePayment transaction).
- Tender Specific and Tender Specify Category (eCheck or credit card; this value controls what will be displayed on SF Institution Set 2 page for an eCheck item type or a credit card item type.

See Also

lssf, Completing Student Financials General Setup, Setting Up Item Types and Item Type Groups

Setting Up Self-Service Payment Messages

To set up self-service payment messages, use the Payment Messages component (SF_PAYMENT_MESSAGE).

Self-service payment messages display to the student when an error is encountered processing a credit card transaction. The credit card processing vendor delivers the codes and default descriptions, but you must define your own message text. This section discusses how to define self-service message text.

Page Used to Set Up Self-Service Payment Messages

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Definition Name</th>
<th>Navigation</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Messages</td>
<td>SF_PAYMENT_MESSAGE</td>
<td>Set Up SACR, Common Definitions, Self Service, Student Financials, Self-Service Payment Messages, Payment Messages</td>
<td>Define self-service message text. Used for self service, application center, and cashiering.</td>
</tr>
</tbody>
</table>

Defining Self-Service Message Text

Access the Payment Messages page (Set Up SACR, Common Definitions, Self Service, Student Financials, Self-Service Payment Messages, Payment Messages).
Chapter 1  Setting Up ePayment Processing

Payment Messages page

**Code**
Valid payment message codes are delivered by the credit card processing vendor and must not be modified. As new codes are made available by the vendor, you may add them to the list, but you must not create and add your own codes.

**Description**
You can modify the entries listed in this column to have up to a 30-character short description. The descriptions that you enter in this column are for internal use only. Students making a payment over the internet do not see these descriptions.

**Note.** The default description for each authorization reply code is identical to the code itself.

**Message Text**
Enter the message text you want the system to display to students based on the authorization reply code sent by the credit card processing vendor. Unless text is entered, students receive an error indicator but no message. If you want students to contact you regarding certain credit card problems, this is where you enter that information.

**Delivered Valid Payment Message Codes**
The following table lists the payment message codes delivered with your system:
<table>
<thead>
<tr>
<th>Code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAVSNO</td>
<td>The bank accepts the credit card, but the credit card processing vendor did not because the credit card did not pass the Address Verification System (AVS) check. The AVS result is no.</td>
</tr>
<tr>
<td>DCALL</td>
<td>You must call the payment processor to proceed with the transaction.</td>
</tr>
<tr>
<td>DCARDREFUSED</td>
<td>The bank declined the transaction.</td>
</tr>
<tr>
<td>DDISTDENY</td>
<td>A distributor denied the request to sell a particular product.</td>
</tr>
<tr>
<td>DINVALADDRESS</td>
<td>The city, state, or postal code entered was invalid.</td>
</tr>
<tr>
<td>DINVALDADDRESS</td>
<td>The credit card number did not pass the credit card processing vendor’s basic checks.</td>
</tr>
<tr>
<td>DINVALIDDATA</td>
<td>The data provided was not consistent with the request. For example, a student may have requested a product with negative cost, or an electronic license certificate (ELC) for a physical product.</td>
</tr>
<tr>
<td>DINVALIDPROD</td>
<td>Not enough information was provided to generate the download URL.</td>
</tr>
<tr>
<td>DMISSINGFIELD</td>
<td>The request contained an unpopulated required field.</td>
</tr>
<tr>
<td>DNOAUTH</td>
<td>A request was made to bill an order for which there is no corresponding, unused authorization record. This occurs if there was not a previously successful ics_auth request or if the previously successful authorization has already been used by another ics_bill request.</td>
</tr>
<tr>
<td>DNOBILL</td>
<td>A request was made to credit an order for which there is no recorded billing code.</td>
</tr>
<tr>
<td>DNTFDECLINED</td>
<td>The bank declined the transaction. For IBM Global Merchant (NetTrade Finance) customers only.</td>
</tr>
<tr>
<td>DPARSEADDRESS</td>
<td>The credit card processing vendor could not interpret the address information.</td>
</tr>
<tr>
<td>DRESTRICTEDE</td>
<td>One of the following problems may have occurred:</td>
</tr>
<tr>
<td></td>
<td>• The end user is on the U.S. List of Denied Countries or the U.S. List of Denied Persons.</td>
</tr>
<tr>
<td></td>
<td>• The ship-to country is in the U.S. Government denied countries list (CU, IR, IQ, LY, KP, SD, SY).</td>
</tr>
<tr>
<td></td>
<td>• The merchant supplied an export list for one or more of the offers in the order, but the shipping country the end user submitted is not in that list.</td>
</tr>
<tr>
<td>Code</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DSCORE</td>
<td>The score exceeds the limit.</td>
</tr>
<tr>
<td>ESYSTEM</td>
<td>A system error occurred. You must call your credit card processing vendor.</td>
</tr>
<tr>
<td>ESTIMEOUT</td>
<td>For ics_auth, if an auth was approved, it is not reversed. For ics_bill, during code cleanup an ics_credit is issued to balance out the ics_bill. For ics_credit, during code cleanup an ics_bill is issued to balance out the ics_credit.</td>
</tr>
<tr>
<td>FAMOUNTHIGH</td>
<td>The amount of the transaction requested is too high for the credit card processing vendor.</td>
</tr>
<tr>
<td>FAMOUNTLOW</td>
<td>The value entered in the amount field was not greater than zero.</td>
</tr>
<tr>
<td>FCONNECTION</td>
<td>The connection failed. The merchant ID and configuration must be checked.</td>
</tr>
<tr>
<td>FDECRYPT</td>
<td>Credit card decryption failed.</td>
</tr>
<tr>
<td>FINITIFAILLED</td>
<td>A vendor error occurred. ICS_INIT failed.</td>
</tr>
<tr>
<td>FINVALIDADR1</td>
<td>The value entered for Address 1 was not valid.</td>
</tr>
<tr>
<td>FINVALIDCARD</td>
<td>The credit card number entered was too long.</td>
</tr>
<tr>
<td>FINVALIDCTRY</td>
<td>The country entered was not valid.</td>
</tr>
<tr>
<td>FINVALIDCURR</td>
<td>The currency was not valid.</td>
</tr>
<tr>
<td>FINVALIDEMAIL</td>
<td>The email address entered was not valid.</td>
</tr>
<tr>
<td>FINVALIDPHON</td>
<td>The phone number entered was not valid.</td>
</tr>
<tr>
<td>FINVALIDSERV</td>
<td>The service requested was not valid.</td>
</tr>
<tr>
<td>FINVALIDSTAT</td>
<td>The length of the state field was not valid.</td>
</tr>
<tr>
<td>FINVALIDZIP</td>
<td>The zip code entered was not valid.</td>
</tr>
<tr>
<td>FREFUNDError</td>
<td>The refund amount exceeded the amount settled.</td>
</tr>
<tr>
<td>FRQIDMISSING</td>
<td>The request ID is required for settlement.</td>
</tr>
<tr>
<td>FSENDFAILED</td>
<td>A vendor error occurred. ICS_SEND failed.</td>
</tr>
<tr>
<td>NMERCERR</td>
<td>The transaction ran without a merchant_id.</td>
</tr>
<tr>
<td>SOK</td>
<td>The transaction was successful.</td>
</tr>
</tbody>
</table>
Setting Up Self-Service Options

You can use self-service options to define business unit labels for self-service payment pages. The values you enter here are used in the View By column headings on self-service pages.

See lsss, Setting Up Student Financials Self Service, Setting Up Self-Service Options.