

PayFlow Link™ Secure for Miva Merchant™

*Security Enhanced PayFlow Link™
Integrated With VeriSign's Fraud
Protection Services*

Product Manual



Table of Contents

Module Description	3
Key Benefits.....	3
Theory of Operation.....	5
General Theory	5
Module Theory.....	9
Module Installation and Upgrading	13
Domain Installation of Module.....	13
Silent Post Return Handler.....	14
Store Installation of Module	15
Module Upgrading.....	17
Module Usage.....	19
Module Configuration.....	19
Payment Module Configuration.....	20
VeriSign Manager Configuration	22
Legal Information	23
Copyright Information	23
Corporate End User License Agreement	24



Module Description

The PayFlow Link™ Secure Payment module for Miva Merchant provides the most secure and reliable payment processing available using the VeriSign™ PayFlow Link gateway. By utilizing behind-the-scenes communications with VeriSign servers, the module provides enhanced protection to the vendor against fraudulent transactions and also allows the vendor to *reliably* utilize the Accepted URL security features of the VeriSign Manager™. With integration support for VeriSign's Fraud Protection Services™, this payment module provides security and peace of mind to the Internet Vendor.

Key Benefits

- Standard VeriSign PayFlow Link Features:
 - Choose either Immediate Sale or Delayed Capture transactions
 - Accept Visa, MasterCard, American Express, Diners' Club, Discover, JCB and Echeck transactions
- Advanced Card Validation and Processing Features:
 - Enhanced pre-processing validation – pre-validates card numbers using known card prefix codes and mod10 calculations to ensure card numbers meet validation rules before being transmitted to VeriSign.
 - Sites look more professional – *customers do not leave the Miva Merchant store to perform payment processing!*
- Advanced Security Features:
 - Works with **VeriSign's Fraud Protection Services** for the highest level of fraud protection. Fraud filters can be configured in your VeriSign Manager; works with both Automatic Decline and "Under Review" fraud protection configurations.
Note: Storeowner must enroll in VeriSign's Fraud Protection Services separately.
 - Provides **secure HTTPS** silent post **TO** and **FROM** VeriSign servers
 - Provides for **secure and reliable** use of the VeriSign Manager Accepted URL feature
 - **Hides** the VeriSign Manager Vendor Login and Partner from customers – prevents carding attacks
 - Utilize **Card Security Codes (CSC)** for fraud protection
 - Utilize **Address Verification Service** for fraud protection and lower IMA discount rates
- Advanced Error Reporting Features:
 - Customers receive clear and understandable error messages when payments are declined for any reason including AVS or CSC failures
 - Configurable error messages for AVS and CSC failures
 - Utilizes Silent Post Back feature of VeriSign Manager to report true error codes



-
- Enhanced Display and VeriSign Manager Reporting Features:
 - Customizable data entry help messages
 - Customizable special instructions that appear on payment pages
 - Customizable PayFlow Link COMMENT1 Field, defaults to order number – the COMMENT1 field displays in many standard reports providing simple and immediate visual indication of what order number a transaction corresponds to.
 - Customizable PayFlow Link COMMENT2 Field, defaults to customer login and IP address – the COMMENT2 field displays in many standard reports providing simple and immediate visual indication of what customer a transaction corresponds to. The IP address of the customer is provided for further fraud identification.
 - Customizable PayFlow Link Order Invoice Description field (DESCRIPTION).
 - Sends Shipping & Tax amounts to PayFlow Link for improved VeriSign Manager reports



Theory of Operation

General Theory

Secure online and real-time payment processing is the single most important aspect of E-commerce. The security aspects of Internet commerce are not only designed to protect the shopper, but also the storeowner. Not all payment modules behave the same, and not all payment modules and gateways provide the optimum level of security for both the shopper **and** the storeowner.

Security measures taken for the benefit of the shopper generally include the use of encryption technology to secure communication between the client (web browser), the host server (E-Commerce site) and the payment gateway, and ensuring credit card numbers are not stored unencrypted on the host server. These security measures generally ensure that the customer's credit card information cannot be stolen and used for fraudulent purposes. Under proper conditions, shopping from an E-Commerce site can be more secure than shopping at a normal brick-and-mortar store, as an employee of the store can become another source of credit card fraud. When encryption technology and real-time payment processing are employed correctly through an online gateway, the E-Commerce store and employees of the business never have the opportunity to view the credit card number being processed.

Security measures taken for the benefit of the storeowner generally include the use of customer validation algorithms such as the use of an Address Verification Service (AVS) and Card Security Codes (CSC) to prevent a fraudulent credit card transaction. Encryption technology and special algorithms are utilized to ensure that an unscrupulous customer does not alter order information and payment gateway processing results during transaction processing. Further, many gateways can provide special fraud screening algorithms during card processing to protect the storeowner from fraudsters.

Types of Payment Modules for Miva Merchant

Payment modules for Miva Merchant (and for E-Commerce in general) can be divided into two primary classifications of modules as determined by the method of communications used between the online store and the payment gateway. These two different classifications provide the storeowner with differing levels of security and ease of use; the developer with differing levels of integration complexity; and the shopper with different levels of security and usability.

Gateway Link (HTML Forwarding) Payment System

A gateway link module is generally used to provide a simple card-processing interface to the customer and is typically easier to integrate into a shopping cart as a software developer. The primary characteristic of a Gateway Link module is that the customer is forwarded to a different web site to perform payment processing. *The standard PayFlow Link module for Miva Merchant used with the PayFlow Link payment gateway is an example of a Gateway Link Payment System.*



Payment processing is generally accomplished by the store by providing a special order form that sends the submission data directly to the gateway web server; the customer payment information is not sent to the originating store. Following completion of the payment processing, the customer is then directed back to the originating store to view their invoice via another form or HTML link from the payment-processing site.

When used with the SSL encryption technology built into all standard web browsers and servers, Gateway Link modules can provide **maximum security to the shopper** by ensuring the credit card data is never sent directly to the merchant, and that the credit card information is never transmitted over the Internet in an insecure fashion. However, Gateway Link modules **provide less than optimal security to the merchant**. Since the customer is provided an HTML page that posts the transaction information to the external payment gateway site, the customer can view and potentially alter the payment information sent to the gateway. Further, the traditional method of transmitting the success codes from the payment gateway back to the originating store is again via HTML Link (or HTML POST) from the customer's web browser. Since this operation is in the hands of the shopper, **opportunities exist for alteration of the return codes** or forging them altogether, and for return codes to be lost in the event the shopper does not click on the return link following payment processing.

Further, since the information required for processing a payment is provided in an HTML web form for the customer to submit, **all** information necessary to run transactions through the gateway is presented to the shopper; this puts the merchant at risk of a **carding attack** where a fraudster utilizes the merchant's payment gateway information for testing stolen credit card numbers for validity. Often, when a fraudster performs a carding attack, the **merchant is held responsible for all transaction fees associated with the carding attack**.

Note: Some gateways, including the VeriSign PayFlow Link Gateway provide methods for silent-post back of order confirmation data. While this does provide an additional level of security, it does not protect the storeowner from carding attacks. Further, if the implementation details are known, it is still possible to forge a silent-post back and create a fraudulent order in the shopping cart.

Direct Communication Payment System

The primary characteristic of a direct communication module is that all payment processing communication occurs behind the scenes using direct encrypted communication with the payment gateway. Since the host server handles all communications with the gateway, there is very little opportunity for a hacker to manipulate or forge any communications data. To do so would require compromising the communications layer between the host server and the gateway system, a more sophisticated attack that is beyond the scope of security within the payment module or payment gateway. *The PayFlow Pro module for Miva Merchant used with the PayFlow Pro payment gateway is an example of a Direct Communication Payment System.*



Payment processing is handled entirely with the store by the shopping cart software, and the customer never leaves the primary store website.

When used with the SSL encryption technology to secure communications between the host and gateway servers, Direct Communication modules can provide **maximum security to the shopper** by ensuring that credit card information is never transmitted over the Internet in an insecure fashion. However, since the credit card information **is** provided directly to the merchant, the storeowner **must** take measures to ensure that this information is never stored on the host server in a manner in which it could be easily compromised. Generally this is accomplished by using encryption to store credit card numbers when it is necessary to do so, though a more effective manner is to never store the card following receipt of a transaction references number from the gateway system.

Direct Communication modules also **provide optimal security to the merchant**, since the host server manages all payment processing communication.

Fraud Opportunities With Automated Payment Systems – Carding Attacks

Any time an automated payment gateway is utilized for payment processing, opportunities exist for abuse of the automated system. A common abuse of the system is to use an online store or even the payment gateway itself as a source for validating stolen credit card numbers. In this type of attack, commonly known as a “carding attack”, the fraudster will attempt to process a large number of small purchases or transactions over a short period of time using different cards in order to find a card number that is valid and has not yet been cancelled.

Generally, a Gateway Link Payment System that uses an HTML form to permit the shopper to POST the payment data to an external payment gateway exposes the merchant to carding attacks. Since all of the information required to utilize the external gateway **must** be embedded in the form, the customer can view this information and use it at a later date to simulate transactions from the merchant’s website. Often, as is the case with PayFlow Link, the attacker must only know the VeriSign Partner and Login names in order to issue a carding attack. Both of these items are exposed in all traditional module implementations for PayFlow Link. ***The standard PayFlow Link module for Miva Merchant exposes the merchant to a carding attack.*** It is important to note that once a fraudster has determined your VeriSign Partner and Login, they do **not** need to utilize your website or online store in order to proceed with a carding attack. Thus, they can perform this attack without your prior knowledge and you cannot prevent them from continuing to do so in the future.

This module protects the vendor from a direct carding attack since the vendor’s VeriSign Partner and Login are no longer exposed to the customer. Further, a special *secure* referring URL feature of the module (described in the next section) prevents the fraudster from using your VeriSign Partner and Login even if they have been exposed in the past.



A False Sense of Security – The Myth of the “Referring URL”

The VeriSign Manager offers a feature known as the “Accepted URL security feature”. The payment gateway will refuse to process any payment request that did not originate at one of the listed URLs. The following excerpts from the *PayFlow Link User’s Guide* describes the feature in this way:

What security features does PayFlow Link offer?

The Accepted URL security feature stops unwelcome parties from changing the dollar value of amounts being passed through PayFlow Link. If you are concerned about this issue, be sure to check the dollar amount of all transactions in VeriSign Manager, even when using this feature. Accepted URL is described in “Accepted URL Security Feature” on page 30.

On page 30 of the *PayFlow Link User’s Guide*, the following caution is provided:

CAUTION: The Accepted URL feature is designed to assist you, but is not a strong anti-fraud tool. If you are concerned about this issue, be sure to use VeriSign Manager to verify the dollar amount of all transactions.

While this feature **may** prevent an unsophisticated shopper from manipulating the dollar amount of a transaction, **it does not provide any security to the merchant** from the knowledgeable hacker or fraudster. The Referring URL security feature checks the list of accepted URLs against the referring URL value *provided by the web browser*. In other words, the customer (or fraudster) provides this information to VeriSign, not your web server- thus ***the Referring URL can be easily forged and should never be used as a security measure when the information is sent from an unknown location.*** As a corollary, the Referring URL should only be used as a trusted value when the data is sent from a known server or client machine*.

*Note: This corollary will be used in the security mechanisms of this module as described in the module theory below.



Module Theory

This PayFlow Link payment module uses advanced communications and security features to provide the level of security common with Direct Communications Payment Modules, while still utilizing the PayFlow Link payment gateway. It provides security and peace of mind to the merchant that:

1. Their PayFlow Link Partner and Login codes will not be exposed (by the module) to the general public, thus eliminating the possibility of direct gateway carding attacks using their Login.
2. Merchants can *safely and effectively* utilize the Referring URL security feature of the VeriSign PayFlow Manager to further ensure that POST data sent to the VeriSign Gateway originates from their own server. A special security code can be utilized in the Referring URL to provide unparalleled security when posting data.
3. Merchants are protected against fraudulent orders that can be created by customers bypassing the payment gateway and forging a valid return POST. Since the customer never has the opportunity to see the variables sent to VeriSign, they cannot forge proper return values.
4. Customers will be presented with simple and meaningful error messages when a card validation fails for any reason, including CSC and AVS failures.
5. The Merchant can take advantage of the new VeriSign Fraud Protection Services to deploy advanced fraud protection filters for their merchant account. The merchant can choose to automatically decline any transaction flagged by the filters as potentially fraudulent, or the merchant can choose to permit the order to be created and review the payment details prior to shipping the products to the customer.

Securing the Vendor Partner and Login

This module utilizes silent-post communications both to **and** from the VeriSign payment gateway via an encrypted communications channel. Therefore the customer is never shown the necessary variables used to perform a PayFlow Link authorization transaction. The Partner and Login information is thus secured, protecting the vendor from direct gateway carding attacks.

Securing the Referring URL

Since the communication to the VeriSign gateway is performed behind the scenes by the payment module, one can safely assume that a trusted host server has sent the transaction if certain criteria are met. These criteria are:

1. The host server performs the call using a secret Referring URL.
2. All gateway calls are encrypted, thus preventing eavesdroppers from determining the secret Referring URL.
3. The gateway server is deemed to be secure, including physical access to the server Log Files. If you trust VeriSign to process your credit card data securely, it may be reasonable to assume that their servers are reasonably secure as well, and that their staff is reasonably trustworthy with their logging data.



This module allows you to provide a secret Referring URL that will be used to initiate all gateway communications; using the pre-configured “VeriSign Manager Accepted URL” setting from the module as your Accepted URL setting in the VeriSign Manager provides optimal Referring URL security that you can rely on to ensure that all transactions originate from your online store.

Securing the Silent Post Return

This module utilizes a secure handshake mechanism with the VeriSign gateway that includes a transaction specific security token that must be returned from the VeriSign gateway in the Silent Post return. Since the shopper cannot view the security token, the module can validate that the silent post return data is authentic and discard any forged silent post returns. Therefore, it is impossible for a customer to bypass the payment gateway and create falsified orders in your Miva Merchant store. Further, the silent post return data is utilized for error-code processing in order to display concise processing errors to your customers.

Configurable AVS and CSC Failure Messages, Improved Error Reporting

One common difficulty experienced among users of the standard Miva Merchant PayFlow Link integration is when using AVS and/or CSC, customers easily become confused with the results of a transaction that is voided due to AVS or CSC settings. Some of the confusion often occurs as a result of the following configuration guidelines specified in the Miva Merchant guide *HOW TO Set Up Payment Configuration* and how this interacts with the VeriSign PayFlow Link product. The following excerpt appears in the *HOW TO* guide Revision 1.8, page 19 item 8:

<http://www.miva.com/docs/merchant/howto41/MM1023.pdf>

8. Next to Force Silent Post Confirmation, check the box to enable it.

The following excerpt appears on page 92 of the *PayFlow Link User’s Guide*. Pay close attention to the very last sentence, bolded for convenience:

*The Force Silent Post Confirmation option ensures that no transactions proceed unless your Web site receives the Silent Post data. If you enable this feature, PayFlow Link sends the Silent Post data and waits for a 200 Success from your server (indicating the server’s receipt of the data). If PayFlow Link does not receive the success response, then the transaction is voided and the customer sees a communication error message. **In this case, VeriSign Manager displays both a transaction that succeeded and a transaction that was voided.***

While the Force Silent Post Confirmation is desirable when using the standard Miva Merchant PayFlow Link integration, this combination of events that are not unlikely when using Full AVS and CSC settings poses an immediate source of confusion for the customer:

1. The customer sees a successful transaction message, and a hold is placed on the customer’s credit card for the full amount of the transaction.



-
2. Underneath the success message, a secondary error message is provided indicating that a transaction was voided (sometimes accompanied by a communications failure message). **It is often easy for the customer to misread (or not read) the void message, and believe the vendor has actually charged the card.**
 3. No order is created in Miva Merchant. Returning to the Miva Merchant site causes the customer to find that they must still pay for their order- usually resulting in a lost sale. Typically this not only results in a lost sale, but also an angry phone call from the customer who believes the card has been charged and that he will not receive the product.

*This module prevents the confusing scenario above by providing a single, accurate and configurable error message to the customer. When configured for extended error reporting, either the standard or a pre-configured CSC or AVS failure message is presented to the customer. When configured for normal error reporting, the customer will simply see an indication that the card was unable to be processed.**

When configured for extended error reporting, all of the error messages according to Table A-1 on page 75 of the VeriSign PayFlow Link User's Guide will be presented to the customer when appropriate.

*Note: A hold is generally still placed on the card for the full amount of the transaction for approximately 24 hours (until the automatic void is also batched and processed).

Note 2: The configurable error messages are **not used if you are using the VeriSign FPS filters for AVS or CSC. Instead, FPS error messages are shown.



About VeriSign's Fraud Protection Services

The following excerpt is provided from VeriSign, and is used with permission. (Copernicus is a VeriSign Integration Partner.) The full web based help for VeriSign's FPS system can be found at: http://www.verisign.com/support/payflow/manager/WebHelp/fps_help.htm

Online fraud is a serious and growing problem, one that cost merchants an estimated \$1 billion in 2002.

While liability for fraudulent card-present or in-store transactions lies with the credit card issuer, liability for card-not-present transactions, including transactions conducted online, falls to the merchant. As you probably know, this means that a merchant that accepts a fraudulent online transaction does not receive repayment for the transaction and additionally must often pay penalty fees and higher transaction rates. One notable exception, buyer authentication, is discussed in the Buyer Authentication section of the User's Guide.

VeriSign's Fraud Protection Services, in conjunction with your Payflow service's standard security tools, can help you to significantly reduce these costs and the resulting damage to your business.

Important Note: In order to enroll with and use the Fraud Protection Services products, merchants must meet the following eligibility requirements: 1) Merchant must have a current, paid-up VeriSign Payflow ProSM or VeriSign Payflow LinkSM gateway service account, 2) Merchant must be in Live mode (activated) with the gateway service, 3) Merchant must have its business operations physically based in the United States, 4) Merchant must use a terminal-based processor supported by the VeriSign PayflowSM gateway.

This module is designed to work with VeriSign's FPS for PayFlow Link. However, Copernicus cannot offer advice or assistance in configuration of your VeriSign Manager and Fraud Protection Services account. Please contact VeriSign or your VeriSign partner for assistance in purchasing and configuring FPS in your VeriSign Manager.



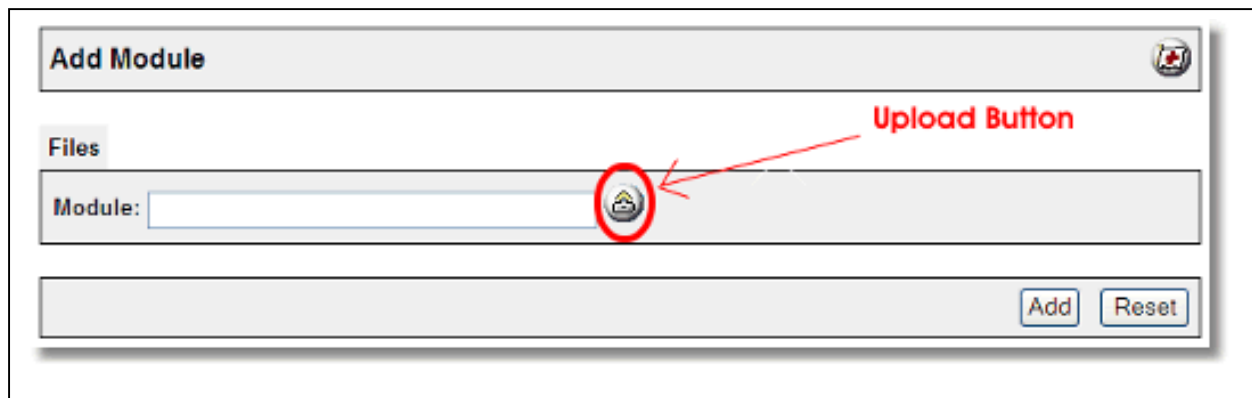
Module Installation and Upgrading

Domain Installation of Module

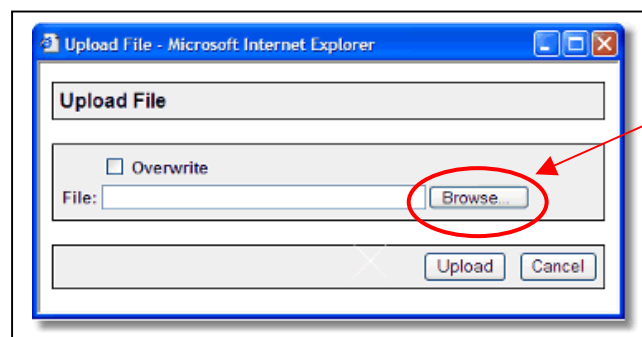
You must first install the module in your Miva Merchant domain. After that you will need to follow the steps for installing the module in the store for which you have purchased the license.

Module Domain Installation

1. Go into the Miva admin (*admin.mv*)
2. Open the **Modules** branch
3. Click on the **Add Module** link and the screen pictured below will appear
4. Click the **Upload** button



5. A Pop-Up window, like the one pictured below, appears and allows you to either **Browse** to find the module on your local drive or enter the filename of the module.
(*super_paylink.mv/c*)



6. Press the **Upload** button



7. Once you press the Upload button, the Upload File PopUp box disappears and the Add Module box is again visible. Press the **Add** button

7. Now the module has been installed in the domain. Next you need to install the module in the store

6. This is the Upload button

7. This is the Add button

Silent Post Return Handler

The Silent Post feature of the VeriSign PayFlow Link gateway is utilized for extended error reporting and is required when using VeriSign's Fraud Protection Services. If you would like to utilize the extended error reporting features of this module or if you use FPS, you will need to install the supplied return-handler script on your server with FTP. You should FTP the file to your Merchant2 source directory. FTP the following script depending on what version of Miva Merchant you are using. This file should be FTP'd in Binary Mode in order to ensure it is not corrupted during transfer:

- Uncompiled Miva Merchant 4.00-4.13: super_paylinkp.mv
- Compiled Miva Merchant 4.14+: super_paylinkp.mvc



Store Installation of Module

1. Go to the Miva admin (*admin.mv*)
 2. Open the **Stores** branch
 3. Click on the arrow next to the store name
 4. Click on **Payment Configuration**
 5. Check the checkbox next to the module name. (For this module it is *CBS – PayFlow Link Secure*)
 6. Press the **Update** button at the bottom of the screen.
- 5. Click the checkbox next to the module name**

Payment Configuration	
Modules	CBS - PayFlow Link™ Secure with Fraud Protection Services
Assigned Module	
<input checked="" type="checkbox"/>	CBS - PayFlow Link™ Secure with Fraud Protection Services
<input type="checkbox"/>	Miva Payment
<input type="checkbox"/>	PayQuake
<input type="checkbox"/>	U.S. Merchant Systems
<input type="checkbox"/>	R-P-G (Rodopi Payment Gateway)
<input type="checkbox"/>	E-Commerce Exchange/QuickCommerce 3.0 Payment Gateway
<input type="checkbox"/>	PayPal Instant Payment Notification
<input type="checkbox"/>	Verisign Payflow Pro (PaymentNet)
<input type="checkbox"/>	Verisign Payflow Link

7. A license screen appears that looks like the picture below. Enter the *PayFlow Link Secure* license key you got when you purchased the module license.
8. Read the *License Agreement*
9. Check the box next to **I ACCEPT THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT**
10. Press the **Update** button. Now you have successfully installed the module in the storefront and you are ready to use it!



7. Enter the license key here

9. Accept the license agreement here

10. Press the Update button to save



Module Upgrading

Copernicus publishes updates to its modules when there are significant feature enhancements. Copernicus also publishes upgrades to its modules for clients who are moving from uncompiled Miva Merchant to compiled Miva Merchant. Both updates and upgrades are added to the storefront in the same way. Once you have saved the update or upgrade to your local hard drive, please follow these instructions to add them to your storefront.

Domain Module Upgrading

1. Go to the Miva admin. (*admin.mv*)
2. Open the **Modules** branch
3. Click on **CBS – PayFlow Link™ Secure** module
4. Click on the **Files** link in the content area of the screen

4. Click on the Files link

Edit Module: CBS - PayFlow Link™ Secure with Fraud Protection Services

Information **Files**

Type of Module:	Payment Processing
Code:	CBS-PFLINK
Name:	CBS - PayFlow Link™ Secure with Fraud Protection Services
Provider:	Copernicus Business Systems, LLC -- http://www.cbstech.com/
Version:	4.5
Usage Count (Number of Stores):	1

Active


Update Delete Reset



5. Click the **Upload** graphic button

Edit Module: CBS - PayFlow Link™ Secure with Fraud Protection Services

[Information](#) [Files](#)

Module: 

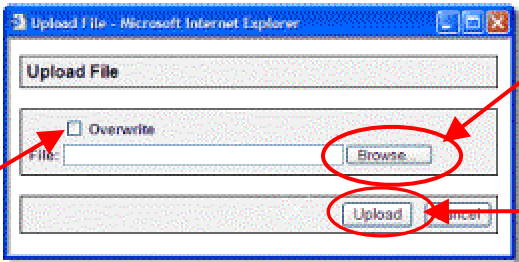
5. Click on the **Upload** button

6. The Upload file PopUp box will appear. Check the **Overwrite** box so that the updated module will overwrite the old version.

6. Check the Overwrite checkbox

7. Click the Browse button to find the file.

8. Press the Upload button




7. Enter the filename of the module on your local drive or use **Browse** to find the file.
8. Press the **Upload** button this will take you back to the “Files” screen.
9. Press the **Update** button and you are finished!

9. Press the **Update** button

Edit Module: CBS - PayFlow Link™ Secure with Fraud Protection Services

[Information](#) [Files](#)

Module: 



Module Usage

Module Configuration

Once you have installed the PayFlow Link Secure payment module, you'll want to configure it. The administrative interface for this module is located in the Payment Configuration section of the Miva admin. To get there follow these steps:

1. Go to the Miva admin (admin.mv)
2. Click the arrow next to **Stores**. This will open up all of the stores you have in this domain.
3. Click on the arrow next to the name of the store in which you have installed this module.
4. Click on the link "Payment Configuration" and in the content area of the Miva Admin you will see all of the tabs specific to the modules installed in this section.
5. Click on the CBS-PayFlow Link Secure tab to configure the module.

Payment Configuration

Modules [CBS - PayFlow Link™ Secure with Fraud Protection Services](#)

Assigned Module	
<input checked="" type="checkbox"/>	CBS - PayFlow Link™ Secure with Fraud Protection Services
<input type="checkbox"/>	Miva Payment
<input type="checkbox"/>	PayQuake
<input type="checkbox"/>	U.S. Merchant Systems
<input type="checkbox"/>	R-P-G (Rodopi Payment Gateway)
<input type="checkbox"/>	E-Commerce Exchange/QuickCommerce 3.0 Payment Gateway
<input type="checkbox"/>	PayPal Instant Payment Notification
<input type="checkbox"/>	Verisign Payflow Pro (PaymentNet)
<input type="checkbox"/>	Verisign Payflow Link



Payment Module Configuration

The payment module is configured much like any other payment processing module. There are two primary configuration sections of this module; the first area at the top of the screen manipulates how the module will behave and what messages the customers will see during checkout. The second section of the module (towards the bottom) is used to configure what types of payments your store will accept (ex: Visa, MC, Echeck, etc.) Each of the settings that manipulate the behavior of the module is described below.

1. **Gateway URL:** <https://payflowlink.verisign.com/payflowlink.cfm>
2. **VeriSign Manager Accepted URL**:**
<http://www.domain.com/securitycode/xxxxxxxxxx>
Note: this will be pre-populated with a random security code. You can use the random code or change the URL to any value desired, though the actual URL should not represent a "real" file. Calls to VeriSign will be originated from this URL allowing you to take advantage of the Accepted URL feature of the VeriSign Manager.
3. **User ID:** Insert your VeriSign User ID (Login)
4. **Partner:** Insert your VeriSign Partner ID (Partner)
5. **Transaction Type:** Choose Authorize Only (Capture Later) or Sale (Immediate Capture)
6. **Require CSC for Credit Cards:** Set to YES to collect the Card Security Code
7. **Use Silent Post for Extended Error Reporting:** If set to YES, make sure to install the silent-post handler as described in the Installation section of this product manual.
Note: This is required when using VeriSign's Fraud Protection Services in your PayFlow Link Manager.
8. **VeriSign FPS - Allow "Under Review" Orders:** When using VeriSign's Fraud Protection Services, you can choose to allow payments that trigger a FPS filter to still generate a Miva Merchant Order. The order will be processed in Miva Merchant normally like all other orders, so vendors of soft goods that immediately become available generally should not choose this option unless the specific filter triggered is deemed to be an acceptably low risk filter. To use this option, enable it and specify in your VeriSign Manager any filters that should cause the order to be taken under review.
Note: If you utilize this option, be certain that you manually accept the payment in your VeriSign Manager prior to fulfilling the order, and make sure you reject (and do not ship) any other payments that you deem to be fraudulent.
9. **AVS Failure Message:** Provide a custom error message that your customers will see if their card is valid but the Address Verification fails.
Note: Requires the use of Silent Post for Extended Error Reporting
10. **CSC Failure Message:** Provide a custom error message that your customers will see if their card is valid but the CSC provided is incorrect.
Note: Requires the use of Silent Post for Extended Error Reporting
11. **Credit Card Number Help Message:** Appears on the order payment information screen next to the credit card box. Generally used to provide instructions to the customer on what formats are acceptable.



12. **Expiration Date Help Message:** Appears on the order payment information screen next to the expiration date box. Generally used to provide instructions to the customer on what formats are acceptable.
13. **CSC/CVV2 Help Message:** Appears on the order payment information screen next to the CSC box. Generally used to describe where to find the CSC/CVV2 number on the credit card.
14. **Order Invoice Description:** Used to provide a custom description when sending the order to the PayFlow Link Gateway. This description appears on the customer invoice sent from VeriSign (if you use this feature of the VeriSign Manager).
15. **PFLink Comment 1:** When left empty, the COMMENT1 field for reports in the VeriSign Manager will display the Order Number. Putting any other text in this field overrides the use of the COMMENT1 field.
16. **PFLink Comment 2:** When left empty, the COMMENT2 field for reports in the VeriSign Manager will display the user login name and customer IP address from where the order was originated. Putting any other text in this field overrides the use of the COMMENT2 field.
17. **Check Payment Instructions:** Provides a description field that appears above the order payment fields when the customer selects an ECHECK transaction.
18. **Credit Card Payment Instructions:** Provides a description field that appears above the order payment fields when the customer selects a credit card transaction.

The picture below shows the initial configuration of the payment methods that your store can accept using PayFlow Link. You should remove any forms of payment that you do not accept by selecting the “Remove” checkbox next to the payment method, and clicking Update. The order of the methods displayed in your store can be modified by clicking the Up/Down arrows.

<i>Accepted Methods of Payment:</i>							
Remove ✓+ ✓-	Order	Code	Name	Payment Type	Prefix	Length	
<input type="checkbox"/>	↓	VISA	Visa	CC	4	13,16	
<input type="checkbox"/>	↑↓	MASTERCARD	MasterCard	CC	5	16	
<input type="checkbox"/>	↑↓	AMEX	American Express	CC			
<input type="checkbox"/>	↑↓	DINER	Diner's Club	CC			
<input type="checkbox"/>	↑↓	DISCOVER	Discover	CC	6011	16	
<input type="checkbox"/>	↑↓	JCB	JCB	CC			
<input type="checkbox"/>	↑↓	ECHECK	TeleCheck	ECHECK			



VeriSign Manager Configuration

In order for the special security features of this module to work properly, you should specify the following configuration in your VeriSign Manager after you have configured the module as described above.

1. **Return URL Method:** Set to Link
2. **Return URL:** Set to the secure URL to the store. (This return link is not used.)
ex: `https://www.domain.com/Merchant2/merchant.mvc`
3. **Silent POST URL:** If using extended error reporting, check the box next to this setting and provide a full URL to the return post processing script:
ex: `http://www.domain.com/Merchant2/super_paylinkp.mvc`
4. **Force Silent Post Confirmation:** **UNCHECK** this box and ensure the Failed Silent Post Return URL is **NOT** specified.
5. **Billing Information Required Fields:** Select the desired “required fields” as specified in your Miva Merchant configuration. If you have selected “Require CSC” (item number 6 in the module configuration), ensure you have checked the CSC box in the required fields. Generally speaking, all of the boxes in the Required Fields should be selected.
6. **Billing Information Editable Fields:** **UNSELECT** all checkboxes in this section. You will not be using the PayFlow Link order confirmation page where these editable billing fields appear.
7. **Shipping Information Required Fields:** Select the desired fields. Generally all fields should be required.
8. **Shipping Information Editable Fields:** **UNSELECT** all checkboxes in this section. You will not be using the PayFlow Link order confirmation page where the editable billing fields appear.
9. **Email Receipt to Customer:** Generally speaking, this should be set to NO, since Miva Merchant will send an invoice to the customer upon order completion.
10. **Security Options (AVS):** Optionally configure this (recommended FULL)
11. **Security Options (CSC):** Optionally configure this (recommended FULL)
12. **Security Options Accepted URL 1**:** Set to the full URL specified in your Payment Module Configuration setting #2 above (VeriSign Manager Accepted URL).

Note: The accepted URL should NOT be a “real” URL to a page or script on your server. Instead, this module utilizes a secret “pseudo-URL” as the referring page when sending payment information to the VeriSign PayFlow Link gateway. This pseudo-URL contains a random security code that is secret and only known to this module and your VeriSign Manager. When your module and the VeriSign Manager are configured with identical values (and this value is kept secret**), it is impossible for fraudsters to launch a carding attack using your VeriSign Login (even if this Login has been exposed in the past due to using a different PayFlow Link module).



Legal Information

Copyright Information

This document and the software described by this document are protected by copyright law. (Copyright © 2002 - 2004 Copernicus Business Systems, LLC. All Rights Reserved.) This document and the software described herein are the property of Copernicus Business Systems, LLC. Use of this document and the software is restricted to the specific terms and conditions in the License Agreement associated with the software. Duplication or distribution of this document or portions of this document for uses not covered by the License Agreement is not allowed without a written agreement signed by an officer of Copernicus Business Systems, LLC. Information contained within this document is subject to change without notice.

THE SOFTWARE DESCRIBED IN THIS DOCUMENT WAS DESIGNED TO SUPPLEMENT SOFTWARE AND/OR OTHER PRODUCTS PRODUCED AND/OR PROVIDED BY MIVA CORPORATION. COPERNICUS DOES NOT ENDORSE AND IS NOT AFFILIATED WITH MIVA CORPORATION, AND DOES NOT CONTROL MIVA PRODUCTS. COPERNICUS IS NOT RESPONSIBLE OR LIABLE FOR ANY UPGRADES, UPDATES, ENHANCEMENTS OR FUTURE RELEASES OF MIVA CORPORATION SOFTWARE OR PRODUCTS THAT MAY BE INCOMPATIBLE WITH THE SOFTWARE OR RENDER THE SOFTWARE INEFFECTIVE. COPERNICUS DOES NOT WARRANT THAT THE SOFTWARE WILL WORK EFFECTIVELY WITH ANY UPGRADES, UPDATES, ENHANCEMENTS OR FUTURE RELEASES OF MIVA CORPORATION SOFTWARE OR OTHER PRODUCTS.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL COPERNICUS BE LIABLE TO CUSTOMER FOR ANY INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF EITHER CUSTOMER OR A THIRD PARTY AGAINST CUSTOMER (INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR INFORMATION, LOST PROFITS, BUSINESS INTERRUPTION OR OTHER PECUNIARY LOSS) ARISING OUT OF OR IN CONNECTION WITH THIS SOFTWARE OR USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF COPERNICUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL COPERNICUS BE LIABLE FOR DAMAGES FOR ANY CAUSE WHATSOEVER (WHETHER BASED IN CONTRACT, TORT OR OTHERWISE) IN EXCESS OF THE AMOUNT PAID TO COPERNICUS BY CUSTOMER FOR USE OF THE SOFTWARE. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

VeriSign PayFlow Link is a service mark of VeriSign, Inc. OPENxb and Copernicus Business Systems are registered trademarks of Copernicus Business Systems, LLC. The Copernicus Revolution, RMXB Technology, Celestia and related images are trademarks of Copernicus Business Systems, LLC. Miva is a registered trademark of Miva Corporation. Miva Script, Miva Merchant, Miva Empresa, and the Miva Engine are trademarks of Miva Corporation. OpenUI is a trademark of the OpenUI Developer's Consortium. MySQL is a trademark of MySQL AB. All other trademarks are the property of their respective owners.



Corporate End User License Agreement

YOU SHOULD CAREFULLY READ ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT PRIOR TO USING THE SOFTWARE. USE OF THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. COPERNICUS BUSINESS SYSTEMS, LLC (“LICENSOR”) IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY IF YOU ACCEPT THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, ERASE ALL COPIES OF THE SOFTWARE, DOCUMENTATION AND ALL OTHER COMPONENTS OF THE SOFTWARE FROM YOUR COMPUTER’S MEMORY AND CERTIFY TO LICENSOR THAT YOU HAVE DONE SO WITHIN SEVEN (7) DAYS OF DOWNLOADING THE SOFTWARE.

1. **Grant of License.** Licensor hereby grants to you (“Customer”) a non-exclusive, non-transferable license to use the Software solely in accordance with the terms of this Agreement. For the purposes of this Agreement, “Software” means the software programs and documentation accompanying this Agreement and any online documentation. This Agreement permits Customer to use one copy of the Software on one MIVA Merchant Domain (“Domain”) and on one Store within that Domain. Customer may make one copy of the Software for archival and backup purposes. Customer must reproduce and include any copyright and trademark notices, legends and logos on each copy of the Software or diskettes made by Customer. The Software is protected by copyright laws and international copyright treaties and other laws regarding trade secrets and other intellectual property rights. Title and full ownership rights to the Software and any and all copies of the Software remain with Licensor.

2. **Use of Software.** Licensor will provide Customer with a license key to activate the Software. The Software may be used only for, by, and on behalf of Customer. Customer **may not** transfer any of its rights hereunder.

IN NO EVENT MAY CUSTOMER TRANSFER THE SOFTWARE TO ANY PERSON, ENTITY OR OTHER END USER IN VIOLATION OF APPLICABLE U.S. EXPORT LAW, INCLUDING, BUT NOT LIMITED TO, ANY TRANSFER FOR USE OUTSIDE THE COUNTRY IN WHICH IT WAS ORIGINALLY LICENSED.

3. **Term and Termination.** This Agreement may be terminated by mutual consent, or by election of either Customer or Licensor in case of the other’s unremedied material breach. In case of any termination of this Agreement, Customer will immediately return to Licensor all the Software components that Customer has obtained from Licensor and any copies in Customer’s possession, and will certify in writing that all such components and all copies of the Software have been returned or destroyed, and all copies erased from the memory of Customer’s computers.

4. **Disclaimer of Warranties.**

4.1 Licensor does not warrant that the functions contained in the Software will meet Customer’s requirements or that the operation of the Software will be error free. The Software is licensed on an “AS IS” basis. The entire risk as to the quality and performance of the Software is solely with Customer.



4.2 NO OTHER WARRANTIES, EXPRESS OR IMPLIED ARE MADE WITH RESPECT TO THE SOFTWARE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO YOU.

4.3 YOU UNDERSTAND THAT THE SOFTWARE WAS DESIGNED TO SUPPLEMENT SOFTWARE AND/OR OTHER PRODUCTS PRODUCED AND/OR PROVIDED BY MIVA CORPORATION. LICENSOR DOES NOT ENDORSE AND IS NOT AFFILIATED WITH MIVA CORPORATION, AND DOES NOT CONTROL MIVA PRODUCTS. LICENSOR IS NOT RESPONSIBLE OR LIABLE FOR ANY UPGRADES, UPDATES, ENHANCEMENTS OR FUTURE RELEASES OF MIVA CORPORATION SOFTWARE OR PRODUCTS THAT MAY BE INCOMPATIBLE WITH THE SOFTWARE OR RENDER THE SOFTWARE INEFFECTIVE. LICENSOR DOES NOT WARRANT THAT THE SOFTWARE WILL WORK EFFECTIVELY WITH ANY UPGRADES, UPDATES, ENHANCEMENTS OR FUTURE RELEASES OF MIVA CORPORATION SOFTWARE OR OTHER PRODUCTS.

5. **Limitation of Liability**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR BE LIABLE TO CUSTOMER FOR ANY INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF EITHER CUSTOMER OR A THIRD PARTY AGAINST CUSTOMER (INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR INFORMATION, LOST PROFITS, BUSINESS INTERRUPTION OR OTHER PECUNIARY LOSS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL LICENSOR BE LIABLE FOR DAMAGES FOR ANY CAUSE WHATSOEVER (WHETHER BASED IN CONTRACT, TORT OR OTHERWISE) IN EXCESS OF THE AMOUNT PAID TO LICENSOR BY CUSTOMER FOR USE OF THE SOFTWARE. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

6. **Other Restrictions and Limitations**. Customer agrees that (1) it will not copy the Software except as permitted in Section 1; (2) it will not reproduce, deactivate, or bypass any security device supplied with the Software; (3) it will preserve and respect Licensor's copyright and the notice of copyright included in the Software; (4) the Software contains information which is confidential and proprietary to Licensor, and Customer will not disclose or transfer or otherwise provide to any third party all or any part of the Software without the express written consent of Licensor; (5) it will not disassemble, reverse compile or reverse engineer the Software or any portion thereof or otherwise attempt to discover the source code or structural framework of the Software; (6) it will not rent or lease the Software; and (7) it will not modify the Software.

7. **Breach**. Customer will be deemed to be in breach of this Agreement if Customer violates any covenants or obligations imposed on it under this Agreement.

8. **License by U.S. Government**. The Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in 48 CFR 52.227-14



(g)(3)(ii) as applicable. Contractor/Manufacturer is Copernicus Business Systems, LLC, 2545 Haddenham Lane, Smyrna, GA 30082.

9. **General Terms and Conditions.** The terms and conditions of any purchase order or other ordering document issued by Customer in connection with this Agreement which are in addition to or inconsistent with the terms and conditions of this Agreement shall not be binding on Licensor and shall not be deemed to modify this Agreement. This Agreement constitutes and expresses the entire agreement and understanding between the parties in reference to all matters referred to herein and any and all previous agreements, discussions, promises, representations, and understandings between the parties relative thereto are merged herein and superceded hereby. The remedies provided in Section 3 shall be cumulative and additional to any other remedies in law or equity which Licensor may have. This Agreement shall be governed by the laws of the State of Georgia and shall inure to the benefit of Licensor, its successors, and assigns. The sole jurisdiction and venue for any litigation arising out of this Agreement shall be an appropriate federal court in the Northern District of Georgia or a state court located in the Northern District of Georgia. Customer hereby consents to personal jurisdiction in such courts. Sections 4, 5, 6, 8 and 9 shall survive any termination of this Agreement. All rights not specifically granted herein are reserved by Licensor.

10. Customer understands and agrees that by agreeing to this License, You are "opting in" to a mailing list. Copernicus Business Systems will use information supplied by You to contact You with marketing and technical information in a variety of ways including, but not limited to, electronic mail, postal mail, telephone and fax. If You do not wish to receive marketing and/or technical information from Copernicus Business Systems, You may use systems provided by Copernicus Business Systems to "opt out" of the mailing list.