Magento Extension

Hosted Payment Pages V2

November 22nd 2015

Contents

About this guide

This guide describes the specifications of the Magento extension for Telr. The intended audience is the merchant's technical staff or the merchant's system integrator.

Copyright

Introduction

The Telr Magento Extension allows merchants who use the Magento system to take payments via the Telr Hosted Payment Pages. No card details are captured by or stored within the Magento system, so there are no PCI requirements for the store.

When the customer clicks on the 'Process Order' button at the end of the Magento checkout screen, they will be taken to the Telr secure server to enter their card details. The result of the purchase attempt (authorised or otherwise) is sent back to the Magento system to update the order details. The customer is also returned to the store.

The extension has been built for Magento Community Edition, and has been tested with version 1.9.2

Installation

The Telr module is available from the Magento Connect extension marketplace.

This is a free extension, and can be found at:

http://www.magentocommerce.com/magento-connect/telr-payments.html

Completing the installation

In order to ensure the Magento system recognizes the new extension, you will need to perform some cache updates. This is done from within the Magento administration system.

From within the System Menu, Select Cache Management.

Click the 'Flush Magento Cache' button, and wait for that to complete.

Now tick the box next to 'configuration', select 'refresh' from the actions list and click 'submit'.

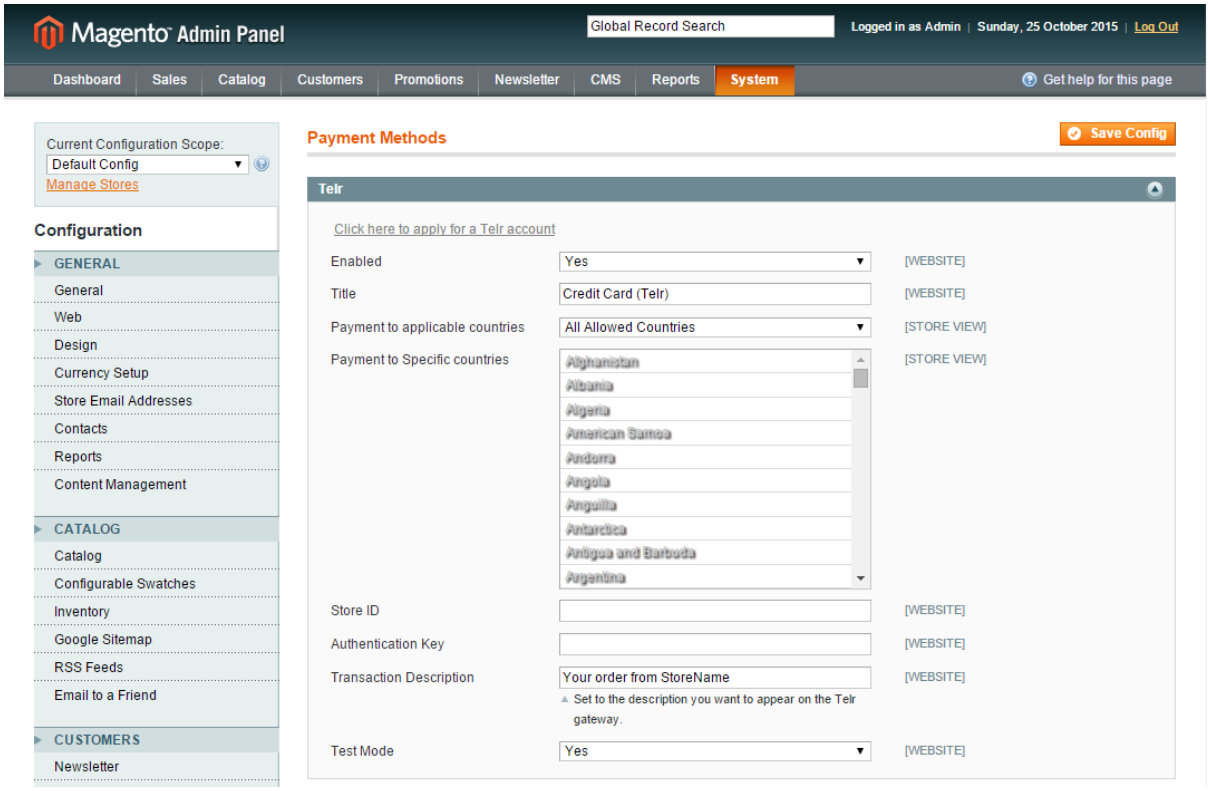
These steps force Magento to re-scan all of the extension options, which will ensure that the extension is made available in the configuration menu.

Configuring Magento

From the System Menu, select Configuration.

Select Payment Methods from the list of configuration options at the side of the page (it is in the Sales section)

Open the Telr Credit Card method and set Enabled to Yes. You also need to set the secret key that has been set as part of your hosted payment page settings. Click the 'Save Config' button to store these changes.



Your Store ID is displayed in the top right of the Telr Merchant Administration System. The authentication key can be found in Telr Merchant Administration System in Hosted Payment Page V2 configuration page, under the Integrations menu.

Payment page customisation

The payment page can be customised through the use of a CSS file. The core page display is based on the BootStrap 3 responsive layout. You should ensure that you are familiar with the underlying styles used within BootStrap before making any CSS changes. For more details please check the Hosted Payment Page integration guide.

Verified by Visa and MasterCard SecureCode

After the consumer enters their card details, the payment gateway will check to see if that card is enrolled as part of the Verified by Visa or MasterCard SecureCode authentication systems (known as 3D-Secure).

If the card is part of one of these authentication systems, then an additional page is displayed which requires the relevant authentication details to be entered. This is usually in the form of a password that has been assigned by the consumer or via a one-time code sent to the customers mobile.

The actual data entry section is presented directly by the card issuer and cannot be customised. It is generally displayed on a white background.

Where possible the 3D-Secure authentication form is displayed over the payment page, allowing the customer to see that it is clearly part of the payment process.

Test Cards

These card numbers can be used when testing your integration to the payment gateway. These cards will not work for live transactions.

Card number	Type	CVV	MPI
4000 0000 0000 0002	Visa	123	No
4111 1111 1111 1111	Visa	123	Yes
4444 3333 2222 1111	Visa	123	Yes
4444 4244 4444 4440	Visa	123	Yes
4444 4444 4444 4448	Visa	123	Yes
4012 8888 8888 1881	Visa	123	Yes
5105 1051 0510 5100	Mastercard	123	No
5454 5454 5454 5454	Mastercard	123	Yes
5555 5555 5555 4444	Mastercard	123	Yes
5555 5555 5555 5557	Mastercard	123	Yes
5581 5822 2222 2229	Mastercard	123	Yes
5641 8209 0009 7002	Maestro UK	123	Yes
6767 0957 4000 0005	Solo	123	No
3434 343434 34343	American Express	1234	No
3566 0020 2014 0006	JCB	123	No

The card security code (CVV) to use with the test cards is 123 (except for American Express, which should be 1234) for an authorised response, other codes will be declined.

Cards which show 'Yes' in the MPI column will use a simulated 3D Secure authentication page, allowing you to test the transaction flow when Verified by Visa or MasterCard SecureCode is used.

Simulating decline/error responses

When it test mode, and when using the above test cards, you can simulate any of the transaction response codes by using specific values for the card security code (CVV). By taking the response code you want to simulate, pad that code with a leading '0' in order to make it a 3 digit code and use that for the CVV.

For example, to simulate the Insufficient Funds response (status 'D', code '41') use 041 as the CVV.

You can also simulate an on-hold transaction in the same way. On hold is where the transaction has been authorised, but the anti-fraud system has flagged the transaction for inspection. Whilst the transaction is on-hold, no funds will be debited from the customers' card. You would need to use the Merchant Administration System to either accept or reject the transaction. To simulate the on-hold response within the test system, use a CVV value of '999' with one of the above test cards.

