worldpay

Requirements for Open Access

Normally, all submissions from merchants to our production systems must originate from a static IP address, for which we sets access permissions in our firewall. Under certain circumstances, we can allow access from non-static IP Address for Online Transaction Processing. Open Access utilizes industry-standard security protection to ensure that your credentials and data are protected when accessing our systems. 128-bit encryption between your endpoint and our server keeps your ID/password confidential, and if access problems occur, we utilize security questions to make sure only you can reset your password. In addition, our systems track logins from new devices and require security questions to proceed, helping to guarantee you have the access you need through quick, safe and reliable means.

In order to take advantage of the Open Access to the production environment, you must meet/conform to the following requirements:

- You must use cnpAPI version V8.14 or above.
- Your Merchant Profile must include the following settings:
  - Maximum Transaction Amount
  - Orphan Refund Limit
  - Transfer Cap
  - Velocity Filters
- You must rotate your password every 365 days (see Presenter Credentials Interface).
- Your HTTP request header cannot contain an **Expect** field.
- Transaction messages are limited to 5000 characters total.
- Supply the email addresses of an Administrator responsible for password rotation, as well as at least one alternate.

> **NOTE:** Worldpay sends email notifications about upcoming password rotations and other information to the Administrator list. Those designated have access to the Presenter Credentials interface.

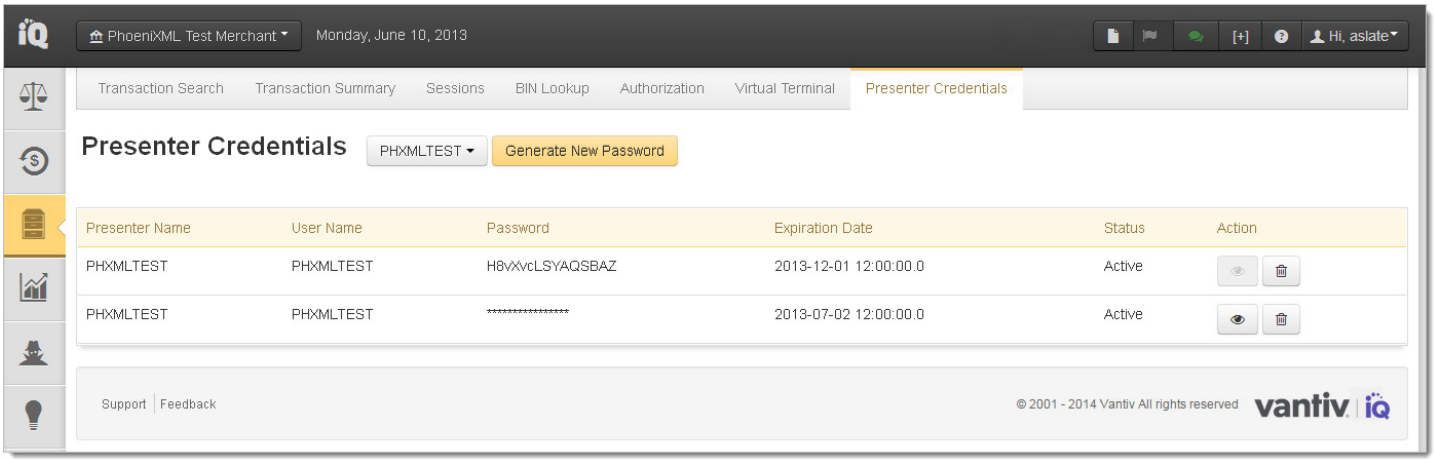
Presenter Credentials Interface

To facilitate the creation of new passwords, we provide the Presenter Credentials interface accessed through iQ. Figure 1 shows an example of the interface immediately following the generation of a new password. Notice in the example that both the new and old password are active. When you generate a new password, by clicking the **Generate New Password** button, the expiration date for the old password either changes to 28 days from the current date or stays as the old expiration day if less than 28 days. The expiration date for the old password will not exceed 28 days. You must complete the password switch-over on your systems prior to the expiration date.

You can never have more than three passwords active at any time. If you have the required privileges, you can deactivate a password immediately by clicking the **Delete** icon in the Action column. The **View** icon in the Action column allows users with the required privileges to view the decrypted/hidden password.

> **NOTE:** If you feel you may not be able to perform the password switch-over on all your systems prior to the expiration date of the old password, please contact your Worldpay Relationship Manager. Manual intervention will be required to extend the life of the old password.
>
> We will reject transaction submitted using expired credentials with a response Value of 3 (see Table 1).

FIGURE 1 Presenter Credentials Interface



Twenty-eight (28) days prior to the expiration of your password we send email notifications to all iQ users that have permissions to view or manage presenter credentials. The emails are sent weekly until within one week of the expiration date. At that point the emails are sent daily until you generate a new password.

Once you have generated a new password, you will receive emails, on the same schedule, reminding you to switch-over the passwords. These emails continue until we no longer receives transactions using the old, expiring password.

Error Messages

When submitting transactions via Open Access, there are HTTP responses and validation errors that may occur. The table below provides information about these responses/error messages.

> **NOTE:** The response value and message in the table represent the values for the **`response`** and **`message`** attributes of either a **`cnpResponse`** or **`cnpOnlineResponse.`**

Response Value	Message	HTTP Status Code / Message	Description	Resubmit?
2	Invalid XML. Contact eCommercesupport@vantiv.com.	200 OK	The submission is not valid XML containing the `user` and `password` elements.	No - debug or contact Worldpay Support
3	Invalid credentials. eCommercesupport@vantiv.com.	200 OK	The submission contains empty or invalid credentials (`user` and `password`).	Maybe - verify credentials
4	Connection limit exceeded. eCommercesupport@vantiv.com.	200 OK	The merchant has exceeded the maximum number of concurrent connections.	Yes
5	Objectionable content detected. Contact eCommercesupport@vantiv.com.	200 OK	The system has determined that the submission may contain objectionable content.	No - debug or contact Worldpay Support
N/A	N/A	405 Method Not Allowed	Only HTTP POST method is allowed.	No - debug or contact Worldpay Support
N/A	N/A	404 Not Found	An invalid URI was used. Verify the URI you are using is correct and that you have not appended any parameters to the URI.	No - debug or contact Worldpay Support
N/A	N/A	417 Expectation Failed	An HTTP **Expect** header was included in the HTTP POST, which is not allowed.	No - debug or contact Worldpay Support