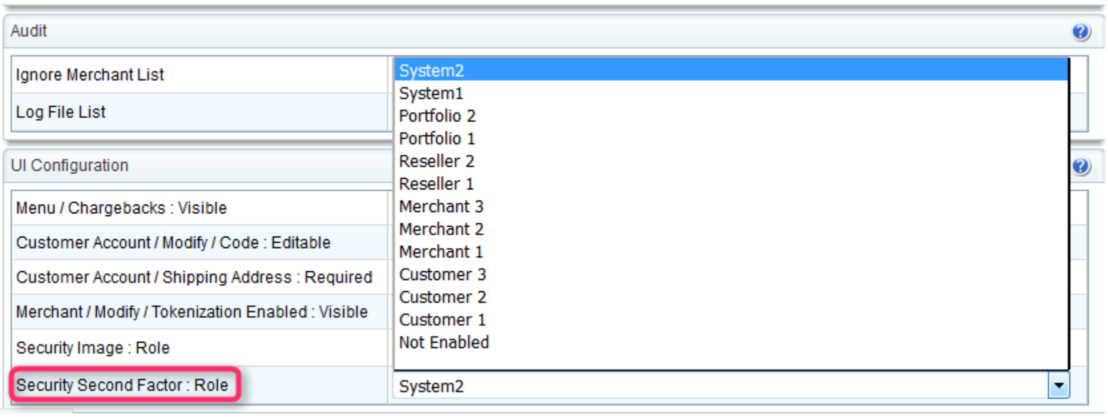
TWO FACTOR AUTHENTICATION GUIDELINES

Two Factor Authentication is a mechanism providing an additional layer of logon authentication with more secure access to the gateway.

To start using the mechanism, it must be enabled on System perspective => Settings => General by entering a user role, for which (and higher) all users will have to have Two Factor Authentication (using Google Authenticator) enabled.



Audit

Ignore Merchant List

Log File List

UI Configuration

Menu / Chargebacks : Visible

Customer Account / Modify / Code : Editable

Customer Account / Shipping Address : Required

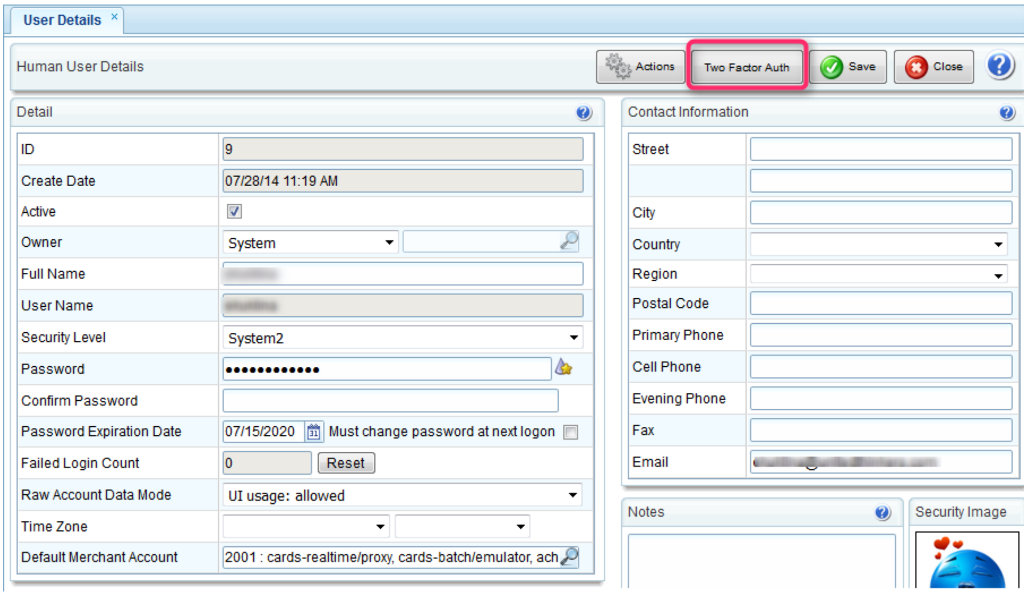
Merchant / Modify / Tokenization Enabled : Visible

Security Image : Role

Security Second Factor : Role — System2

For example, if Portfolio1 role is entered, all users that have roles Portfolio1, Portfolio2, System 1, System2 will be required to use two factor authentication while accessing the gateway from the UI (check all available user roles here: http://www.unipaygateway.info/permissions). All users, for which two factor authentication is applied, will have to install Google Authenticator app on their smartphones.

After that, you have to complete your two factor authentication registration by going to User perspective => Details and clicking on Two Factor Auth button => Register Now:



Detail

ID	9
Create Date	07/28/14 11:19 AM
Active	☑
Owner	System
Full Name	[redacted]
User Name	[redacted]
Security Level	System2
Password	●●●●●●●●●●●●
Confirm Password	
Password Expiration Date	07/15/2020 Must change password at next logon □
Failed Login Count	0 Reset
Raw Account Data Mode	UI usage: allowed
Time Zone	
Default Merchant Account	2001 : cards-realtime/proxy, cards-batch/emulator, ach

Contact Information

Street	
City	
Country	
Region	
Postal Code	
Primary Phone	
Cell Phone	
Evening Phone	
Fax	
Email	[redacted]

Notes

Security Image

In the opened form, you can review the instruction on how to enable two factor authentication for your user account:

Your current security role is **[your role]**. This role requires Two Factor Authentication when you log in, which provides additional security.

When you log in to the site, in addition to your username and password, you will have to provide a six-digit one-time password which will be generated by your mobile phone using Google Authenticator.

In order to generate this one-time password you will have to install the Google Authenticator App. Please follow the steps below to install the app:

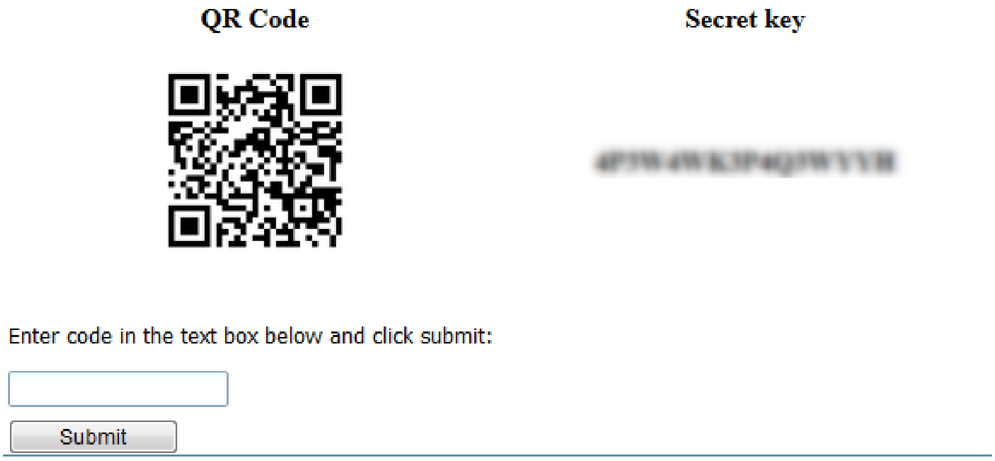
Step 1: Install Google Authenticator on your phone by following these instructions.
https://support.google.com/accounts/answer/1066447?hl=en.

You will need either a QR code or secret key as shown below to complete the set up process You can learn more about Google Authenticator here.

If you have difficulties installing the Authenticator app please contact technical support at **[your-support-email]**.

Step 2: Once you have installed the application, please generate a code and enter it below to complete the registration. Please note that the code is only valid for 30 seconds.

After reviewing the instruction, you will have to enter authentication code. With your Google Authenticator app, you can get it in two ways: either read a QR code or enter the code on the screen. Once you enter the code, your page will be refreshed.



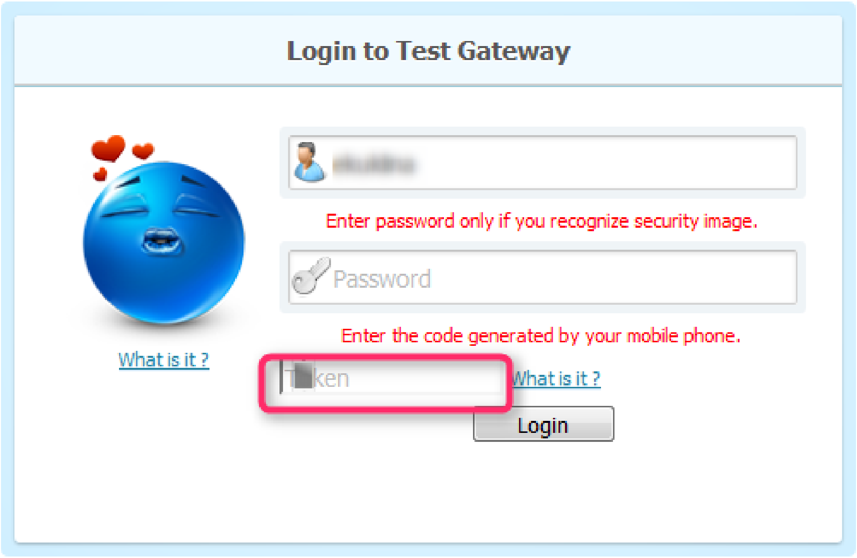
QR Code | **Secret key**

[redacted]

Enter code in the text box below and click submit:

Note if you leave your user account with no Two Factor Authentication activated, the window with activation request will show up. You will have to either complete registration or postpone it. If you select postpone registration option, you will be automatically logged out by the system.

With every single visit after that, for accessing the gateway, you will have to enter a specific token on the logon page. The token will be generated every time when you open Google Authenticator app.



Login to Test Gateway

[redacted]

Enter password only if you recognize security image.

Enter the code generated by your mobile phone.