

PaymentStream[™] AFT

2-Step Security Access for Business Members

December 2017

Central 1 Credit Union 800 661 6813 www.central1.com/thinking.forward 1441 Creekside Drive Vancouver BC Canada v6J 4s7 2810 Matheson Blvd. East Mississauga ON Canada 14w 4x7





Table of Contents

1	Intro	Introduction to 2-Step Security		
2	Hard	Tokens	3	
	2.1	Accessing PaymentStream AFT with a Hard Token	3	
3	Soft	Tokens	4	
	3.1	Installing the Soft Token	4	
	3.2	Installing the Authentication App	5	
	3.3	Accessing PaymentStream AFT with a Soft Token	8	



1 Introduction to 2-Step Security

Business members must be set up with 2-Step Security to access *PaymentStream*[™] AFT. Users can be assigned a Hard Token or a Soft Token. Your financial institution is responsible for assigning security tokens.

2 Hard Tokens

A Hard Token is a physical device that generates a random one-time password when activated. The one-time password refreshes every 60 seconds. A Hard Token is distributed to users by the financial institution.

2.1 Accessing *PaymentStream* AFT with a Hard Token

Users who have received the Hard Token, proceed as follows to access *PaymentStream* AFT:

- Enter the URL provided by your financial institution in the browser address field.
- Enter your User ID and Password.
- Enter the 6-digit code displayed on the Hard Token and select **Done** when completed. See Figure 2.1 and Figure 2.2.



Figure 2.1: 6-Digit Code on Hard Token





Figure 2.2: Enter Code to Access PaymentStream AFT

3 Soft Tokens

A Soft Token is a security token that is installed on the user's mobile device. The Soft Token generates a one-time password every 60 seconds. Soft Tokens must be registered and installed on a user's mobile device within 14 calendar days of the Token being assigned. The device must have an authenticator app installed for the security process to work. Central 1 recommends the Google Authenticator app.

3.1 Installing the Soft Token

To install and register the soft token on your trusted device, proceed as follows:

- Open your browser and enter the URL provided by your financial institution in the address bar.
- Log in to *PaymentStream* AFT with the user ID and one-time password provided by your financial institution.

Users will be prompted to change their one-time password at the first login. The password requirements for *PaymentStream* AFT are as follows:

- must be a minimum of eight (8) characters in length;
- must contain at least one (1) opposite case character;
- must contain at least one (1) non-alphanumeric character;



- must contain at least one (1) numeric character; and
- must not be the same as one of the last 24 passwords used.
- On the Registration page, select **Enable.** To learn more about 2-Step Security, select the information tabs. See Figure 3.1.

Central 1°	0	
ease do not click the back button on your brow	ser as it will close this session and you	will lose your progress.
Register for 2-Step Sec	urity	
Step Security adds an extra layer	of protection to your accour	nt.
Enable		
earn more about 2-Step	Security	
Why it's important	How it works	How it protects you
It is easier than you think for som	neone to steal your passwor	d
Did you know, these common actions could pu	t you at risk of having your password sto	olen:
 reusing the same password on more that Downloading software from the Internet Clicking on links in email messages 	n one site	
2-Step Security can help keep bad guys out, eve	en if they steal your password.	
Is it possible for me to lose acces	s to all my accounts and eve	erything in it?
If a bad guy steals your password, they could in transactions at risk.	ck you out and gain access to your acco	ount(s). This puts your applications and
2-Step Security is a feature that can help keep y	our financial institution protected.	
	Enable	



3.2 Installing the Authentication App

To complete the 2-Step Security process, a mobile authenticator app that supports the RFC 6238 security standard is required. Central 1 recommends Google Authenticator. The



authenticator app will generate a secure one-time passcode, which is required to enable 2-Step Security on the system.

If your mobile device does not have an authenticator app installed that supports the RFC 6238 security standard, proceed as follows:

- Download Google Authenticator from the App store on your trusted mobile device.
- Select **Next** when the app is installed. See Figure 3.2.

Cl Central 1°
Please do not click the back button on your browser as it will close this session and you will lose your progress.
Enable 2-Step Security
To complete the 2-Step Security process you will need an mobile authenticator app that supports the <u>RFC 6238</u> security standard. The sc purpose of the authenticator app is to generate a secure one time passcode. You need this passcode to enable 2-Step Security on our system.
 We recommend downloading the <u>Google Authenticator</u> mobile app. This mobile app will generate the required passcode to complete this process. If you do not have an authenticator app installed on your mobile device, please install it now.
Pack Next

Figure 3.2: Download the Google Authenticator App

- Open Google Authenticator and allow the application to access your camera.
- Use the camera on your mobile device to scan the QR code shown on the left side of the screen. See Figure 3.3.





Figure 3.3: Scan the QR Code with the Google Authenticator App

• Enter the 6-digit code displayed in the app in the Enter Code field. Enter the code without spaces. Select **Next**. See Figure 3.4.



Figure 3.4: Enter the 6-Digit Code from the Mobile Authenticator App

• Select **Done** on the confirmation page. See Figure 3.5.





Figure 3.5: Complete the Registration Process

3.3 Accessing *PaymentStream* AFT with a Soft Token

Users who have installed the Soft Token on their mobile device proceed as follows to access *PaymentStream* AFT:

- Enter the URL provided by your financial institution in the browser address field.
- Enter your User ID and Password.
- Open Google Authenticator on your mobile device and enter the 6-digit code displayed in the app in the Enter Code field. Enter the code without spaces.
- Select **Done.** See Figure 3.6.





Figure 3.6: Enter Code to Access PaymentStream AFT