Testing Multi-Factor Authentication

Introduction
You have been asked to test the new multi-factor authentication (MFA) solution for Valero. Multi-factor authentication means you will be using a device (a token) that generates a one-time password, or OTP, in addition to your regular network login. The one-time password is a six digit number and changes every thirty seconds. This one-time password increases the security of your account because someone can’t login with your account remotely without your one-time password.

You will be assigned a MFA token, otherwise known as a DIGIPASS. There are two versions available, a physical, or hard, token, and a mobile, or soft, token. The hard token is a small device that can be attached to a keychain and has a simple button to press that displays a one-time password. The soft token is an app that you install on a smartphone or tablet and works in the same way the hard token does. You tap the button and it displays a one-time password.

Figure 1: DIGIPASS hard token

Figure 2: DIGIPASS software token

To test MFA, we are asking you to use a special version of the new Go2.valero.com site. Please use this site in place of the regular site while you are testing. During the testing period, you will still be able to switch back to the standard Go2 page if you run into any issues. Email any issues to mfa_testing@valero.com.

You should have received a number of documents as part of this testing. Included should be:

- Mobile DIGIPASS activation instructions
- Installation guide for Citrix Receiver for iOS and Android
• List of scenarios to test

Not all scenarios will apply to you, but please test as many of them as possible. Please submit the completed results to mfa_testing@valero.com.

Activating your DIGIPASS

If you are using a mobile DIGIPASS, you will need to install the application on your smartphone or tablet, then set your PIN. Please refer to the document “How to activate your mobile DIGIPASS” to install the DIGIPASS app.

If you are using a physical DIGIPASS, your DIGIPASS will be ready to use immediately. No additional settings are required.

Logging into the MFA test page

1. Browse to https://go2.valero.com/mfa. The page looks the same as the regular version of go2.valero.com, so make sure the URL is correct:

2. Click on the icon for VPN, Remote Workstation or Valero & Me @ Home. If you are logging in from a tablet or a smartphone, please refer to the Citrix Receiver installation directions for the operating system of your device (iOS or Android).

Choose “VPN” only if you have a Valero-issued laptop to test with.

Choose “Remote Workstation” to test the standard Citrix applications

Choose “Valero & Me @ Home” to test only the Valero & Me application.
How to use your DIGIPASS

1. Regardless of which icon you chose, you’ll be taken to a standard login screen that will ask for your username and password. Enter your username on the line labelled “User Name”.

2. Enter your regular network password on the line labelled “Password”. Click “Log On” to continue.

3. If you entered your username and password successfully, the page will update and now prompt you for your one-time password. Enter your one-time password from your DIGIPASS on the line labelled “Token”. Click “Log On” to continue.
4. After you have entered this successfully, you will log onto VPN, Remote Workstation, or Valero & Me @ Home like normal.

**How to Use a Backup Virtual DIGIPASS**

If you were assigned a physical DIGIPASS and do not have it when you attempt to log in, you can use a feature called the Backup Virtual DIGIPASS (BVDP). This works by entering a special keyword instead of the normal one-time password (OTP) to trigger the system to send you an OTP via email and text message.

To use it, follow these steps:

1. Regardless of which icon you chose, you’ll be taken to a standard login screen that will ask for your username and password. Enter your username on the line labelled “**User Name**”.

2. Enter your regular network password on the line labelled “**Password**”. Click “**Log On**” to continue.

3. If you entered your username and password successfully, the page will update and now prompt you for your one-time password. Instead of entering the one-time password shown on your DIGIPASS, enter the
word “sendotp” (do not include the quotes) on the line labelled “Token”. Click “Log On” to continue.

4. Instead of logging on like normal, you’ll get a prompt for your one-time password. This is normal and expected. Stay on this screen while waiting for step 5.

5. You will get an email to your work email address and a text message to the mobile phone you have listed in the Contacts directory (if you have one listed). In the message will be your OTP.
6. Enter the OTP you received in the field labelled “Enter One-Time Password”. Click “Submit” to continue.

![OTP Entry Form]

7. After you have entered this successfully, you will log onto VPN, Remote Workstation, or Valero & Me @ Home like normal.