Virtual Code Authentication User’s Guide

June 25, 2015
Overview of New Security

Modern technologies call for higher security standards as practiced among many other online systems. Configurable password settings have been in place which allows for sub-standard password practices among users.

As such, you will now go through a two-step log in process.

1. Enhanced Passwords
   - Going forward, your password must contain a minimum of 8 characters and include at least one of the following:
     - Uppercase Letter
     - Lowercase Letter
     - Number
     - Symbol
     - Example: Password1$

2. Multi-Factor Authorization (MFA) or Virtual Code Authentication
   - After you enter your username/password and click login, if the system does not recognize this computer as one you have used in the past 30 days, the system will require a second form of authentication before you can continue. A code will be emailed, texted, or sent to you via an automated voice call, which you will then enter, in order to access the system. The security combination factors are as follows:
     - Password = something you know
     - Code = something you have
Multi-Factor Authentication

Multi-factor authentication requires a user who is requesting access to provide independent authentication factors; a Knowledge Factor, and a Possession Factor.

- Knowledge Factor: Something only the user knows (such as a password)
- Possession Factor: Something only the user has (a code)

One option for the Possession Factor is by virtual code. This works by sending a code to you either by SMS (text message), Voice Call or E-mail. Once the code is received, you will sign in with your username, password and the supplied code. Once correctly entered, you will then be able to login to the system.

The User’s Experience

The first time you login, you will be required to configure the Multi-Factor Authentication settings for future logins.

**Step 1:** Enter Username and Password on the login page.
The Change Password screen will display where the password must be changed to one with the new requirements. The screen will explain the new password standards. Mobile users will also receive this screen.
Step 2: You will then be prompted to configure the Multi-Factor Authentication Settings.

Up to three methods can be configured for receiving your code.

- **SMS Mobile #:** Will be used to send codes via text message (fastest method)
- **Voice Phone #:** Will be used to send codes via voice message
- **Email:** Will be used to send codes via email address

One or more methods may be selected. Any information that is already listed in your account will be pre-populated. If multiple phone or email numbers are stored in the system, those will be made available to you via the drop-down lists shown in each field. You may also enter new information not stored in the system. When this happens, an administrator must approve the new credentials.

Once this step is completed, you will be logged directly into the system.

For any logins thereafter, the code will be delivered via the selected method and is unique to you and will expire in 15 minutes.

Once you enter the code, you can choose to make the computer trusted by checking “Remember This Device” where an encrypted cookie will be placed on the machine for your browser. A trusted computer will not require the 2nd factor again unless the cookie expires or is deleted via the web browser options. It can expire you do not log in for 30 days but the 30 day counter is reset upon every successful login.

Step 3: Anytime thereafter, when logging in from a device that has not been remembered, you will be asked which method you would like to use to receive your code for that specific login. Select a method and click the button to send either Text Message, Voice, or Email.

**NOTE:** It is recommended that you select “Text Message #” as your primary option. The other methods are valid, but due to inconsistencies in email policies and practices (such as Spam/Junk folders, server down-time, etc.), a text message will deliver the code immediately.
Screen to request code:

Please select one of the following methods to validate your identity

Please select one of the following methods to validate your identity. A code will be sent to the method chosen.

You will need to enter this code after you receive it. It should only take a moment to receive it once you’ve made your selection.

Methods: ☐ Text Message ☐ Voice ☐ Email

Text message will be sent to: ******4763 Send Text Message

Enter Code: 

☐ By checking this box, the verification code you enter will be valid on this device for 30 days. If you have not logged in for more than 30 days, you will need to enter a new code.

Continue

Screen after sending the code:

After the code is received, enter the code, check the box* and click “Continue.” You will now be logged in to the system. This option will not show for users who still have approval items pending for the MFA Admin.
If the box is checked, the next time you log in from this device, a second factor of authentication (code) will not be required for login. As a best practice, this option should only be checked on individual personal computers and should never be checked on a public or shared computer.
**Additional Options**

You may change your SMS, Voice and Email settings at any time by navigating to My Account > My Settings > Change Multi-Factor Authentication. If you enter information that is not already stored in the system, an approval will be needed by an administrator.

**NOTE**: This option may or may not be available to you, depending on how your system is configured.